Université de Poitiers

Département de Mathématiques
40 Avenue du Recteur Pineau
86022 Poitiers cedex.

Parcours initiatique à travers la théorie des valuations

Emmanuel Hallouin

MOTS CLES : Valuations - corps locaux - ramification - théorie de Galois - corps complet pour une valeur absolue ultra-métrique

CLASSIFICATION AMS : 11S05 - 11S15 - 11S20 - 12F12 - 12J10 - 12J20 - 12J25 - 13F30

Parcours initiatique à travers la théorie des valuations

Emmanuel Hallouin (hallouin@@mathlabo.univ-poitiers.fr)

Contents

Ce travail a reçu le soutien financier de la région Poitou-Charentes.

Avant propos :

Au tout début de ce travail, la lecture d'un passage d'un livre d'histoire des mathématiques. Il y était expliqué comment Hensel avait été amené à inventer les nombres p-adiques. Peu après, Claude Quitté me conseilla d'écrire une introduction à un éventuel (futur) rapport interne tournant autour des valuations. C'est cette dernière qui figure tout de suite après. Je l'ai laissée telle quelle (alors que toutes les autres sections ont été retouchées de multiples fois) pour insister sur le caractère "initiatique" de ce "parcours". Je pense, en effet, que ce passage témoigne d'une totale naïveté sur le sujet.

Enfin, je viens de faire allusion à un conseil de Claude Quitté ; je tiens à le remercier ici. Sans son aide, ses remarques, et surtout sa perpétuelle envie de transmettre son savoir, d'inévitables incidents de "parcours" m'auraient vite contraint à rebrousser chemin. Pour tout cela, MERCI Claude Quitté.

Introduction

Ce papier, que l'on peut voir comme une introduction à la théorie des valuations, constitue une excursion à travers des domaines satellites de cette théorie : citons l'étude des nombres p-adiques ou plus généralement des corps locaux. Cependant, pour éviter un exposé classique sur ce sujet[1], je voudrais me donner comme fil conducteur un résultat classique de théorie des nombres dont l'énoncé et la démonstration utilisent les objets relatifs à la théorie des valuations. En fait, historiquement, c'est ce même résultat qui a motivé Hensel lui-même à inventer les nombres p-adiques. Plus précisément, le résultat en question concerne la factorisation dans un corps de nombres. Cette factorisation, très convoitée, est aussi une mine d'erreurs (en témoigne celle faite par Kummer). Notamment le fait que tout anneau de nombres ne puisse pas se mettre sous la forme $\mathbb{Z}[\theta]$ rend parfois la tâche du factoriseur ardue. Autrement dit, le théorème de Kummer ne règle pas tous les cas. Cependant, Hensel, à la fin du XIX$^{\text{ème}}$ siècle, découvrit des phénomènes intéressants grâce à son invention : les nombres p-adiques. Tous ces épisodes de l'histoire des mathématiques sont relatés dans le très bel ouvrage "Abrégé d'histoire des mathématiques 1700-1900" [9] dirigé par Jean Dieudonné. Plus particulièrement dans le Chap V, § V, I, les auteurs de cette section, W. et F.Ellison, reprennent le fameux exemple du polynôme de Dedekind, $f(X) = X^3 + X^2 - 2X + 8$ dont on sait que l'anneau des entiers (c'est-à-dire la fermeture intégrale de $\mathbb{Z}$ dans le corps engendré par une racine de f) ne peut pas se mettre sous la forme $\mathbb{Z}[\theta]$. Je laisse la parole aux auteurs :

> *En étudiant des exemples de cette sorte, Hensel (ou plus probablement Kronecker, dont Hensel était l'élève) observa le curieux fait suivant. Supposons que f soit le polynôme minimal de $\theta \in \mathcal{O}$ et que $p \mid C(\theta)$ (l'indice) ; alors la factorisation de $f(x)$ modulo p ne reflète pas nécessairement celle de p dans $\mathcal{O}$; mais il existe un entier $R \geqslant 1$ tel que la factorisation de $f(x)$ modulo p^R indique en quelque sorte la façon dont p se factorise dans $\mathcal{O}$.*

Dans l'exemple de Dedekind, si θ est une racine de f et si $\mathcal{O}$ est la clôture intégrale de $\mathbb{Z}$ dans $\mathbb{Q}[\theta]$, on montre (de manière assez élémentaire) que 2 se factorise en trois idéaux premiers distincts :

$$\langle 2 \rangle = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \quad \text{avec} \quad \mathcal{O}/\mathfrak{p}_i \simeq \mathbb{F}_2$$

Du point de vue polynomial, f vérifie :

$$f(X) \equiv X^2(X+1) \mod 2 \ ;$$

alors que :

$$f(X) \equiv (X-1)(X-2)(X-4) \mod 8.$$

Comme 4 divise $\mathrm{dis}(f)$ mais que 8 ne le divise pas, les trois facteurs modulo 8 reflètent les trois premiers distincts au dessus de 2. Pour comprendre cela, on peut procéder en deux grandes étapes : tout d'abord, il faut faire le lien entre la factorisation de f dans $\mathbb{Z}_p[X]$ (f n'a aucune raison de rester irréductible dans $\mathbb{Z}_p$) et celle modulo une assez grande puissance de p. Ceci est l'objet de toute la section concernant le lemme de Hensel et ses corollaires. On utilise donc déjà l'un des résultats les plus fondamentaux concernant les corps complets pour une valeur absolue ultra-métrique. Ensuite il faut s'attacher à mettre en évidence la correspondance suivante :

Proposition 1 *Soit $f \in \mathbb{Z}[X]$ un polynôme unitaire irréductible, K le corps de nombres engendré par une de ses racines. On considère p un premier de $\mathbb{Z}$. Alors, il y a une correspondance bi-univoque entre les facteurs irréductibles de f dans $\mathbb{Z}_p[X]$ et les idéaux premiers de l'anneau des entiers de K au dessus de p (ou tout simplement de K par abus de langage).*

On peut énoncer un résultat beaucoup plus précis que le précédent (c.f. les sections I.4.5 et I.4.6). Cependant, en guise d'introduction, il est intéressant d'esquisser la trame de la démonstration de ce résultat histoire de se familiariser avec le sujet et de poser les premières notations.

On considère $f \in \mathbb{Z}[X]$ unitaire et irréductible. Soit $K = \mathbb{Q}[X]/\langle f \rangle$ le corps de nombres engendré par une racine de f et $\mathcal{O}$ l'anneau des entiers de K, i.e. la fermeture intégrale de $\mathbb{Z}$ dans K. On choisit un premier p de $\mathbb{Z}$ fixé une fois pour toutes. L'anneau des entiers p-adiques est noté $\mathbb{Z}_p$; son corps des fractions, i.e. le corps des nombres p-adiques est noté $\mathbb{Q}_p$. On rappellera brièvement la construction de ce corps à partir de la valeur absolue p-adique $|\ |_p$ définie sur $\mathbb{Q}$. Cela étant, f est sans facteur carré dans $\mathbb{Z}[X]$

[1] Ceci ne présenterait qu'un maigre intérêt puisque de nombreux livres d'algèbre l'ont déjà fait ; on peut par exemple citer [14], [16], [23], [2], [6], ou évidemment [3], sans oublier [21] dont le titre, "Corps locaux", est plus qu'évocateur...

(puisqu'irréductible !), il le reste donc dans $\mathbb{Z}_p[X]$. En revanche, il n'a aucune raison d'être irréductible dans $\mathbb{Z}_p[X]$. Considérons $g \in \mathbb{Z}_p[X]$ un diviseur irréductible de f dans $\mathbb{Z}_p[X]$. Dans un premier temps, on veut associer à g un premier $\mathfrak{p}$ de $\mathcal{O}$ (ou de K par abus de langage) au dessus de p. Pour cela, on considère la $\mathbb{Q}_p$-extension $E = \mathbb{Q}_p[X]/\langle g\rangle$; c'est une $\mathbb{Q}_p$-extension de degré fini (de degré $\deg g$). C'est aussi une K-extension, c'est-à-dire en revenant aux définitions de K et E :

$$\mathbb{Q}[X]/\langle f\rangle \hookrightarrow \mathbb{Q}_p[X]/\langle g\rangle.$$

En effet, l'idéal $\mathbb{Q}[X]\cap g\mathbb{Q}_p[X]$ est un idéal premier de $\mathbb{Q}[X]$ contenant $f\mathbb{Q}[X]$ donc $f\mathbb{Q}[X] = \mathbb{Q}[X]\cap g\mathbb{Q}_p[X]$. Par suite, $\mathbb{Q}[X]/\langle f\rangle$ s'injecte dans $\mathbb{Q}_p[X]/\langle g\rangle$. L'étude des extensions de degré fini d'un corps complet pour une valeur absolue nous permet de montrer (grâce à l'analyse !) que $\mathcal{O}_E$, la fermeture intégrale de $\mathbb{Z}_p$ dans E, est un anneau local. C'est même un anneau de valuation discrète ; nous y reviendrons. En résumé, on a les deux situations symétriques suivantes :

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\text{clot. int.}} & \mathcal{O} \\ {\scriptstyle\text{Frac}}\downarrow & & \downarrow{\scriptstyle\text{Frac}} \\ \mathbb{Q} & \xrightarrow[\text{ext. alg.}]{} & K \end{array} \qquad \text{et} \qquad \begin{array}{ccc} \mathbb{Z}_p & \xrightarrow{\text{clot. int.}} & \mathcal{O}_E \\ {\scriptstyle\text{Frac}}\downarrow & & \downarrow{\scriptstyle\text{Frac}} \\ \mathbb{Q}_p & \xrightarrow[\text{ext. alg.}]{} & E \end{array}$$

avec les inclusions :

$$\mathbb{Z}\subset\mathbb{Z}_p, \quad \mathbb{Q}\subset\mathbb{Q}_p, \quad \mathcal{O}\subset\mathcal{O}_E \quad \text{et} \quad K\subset E.$$

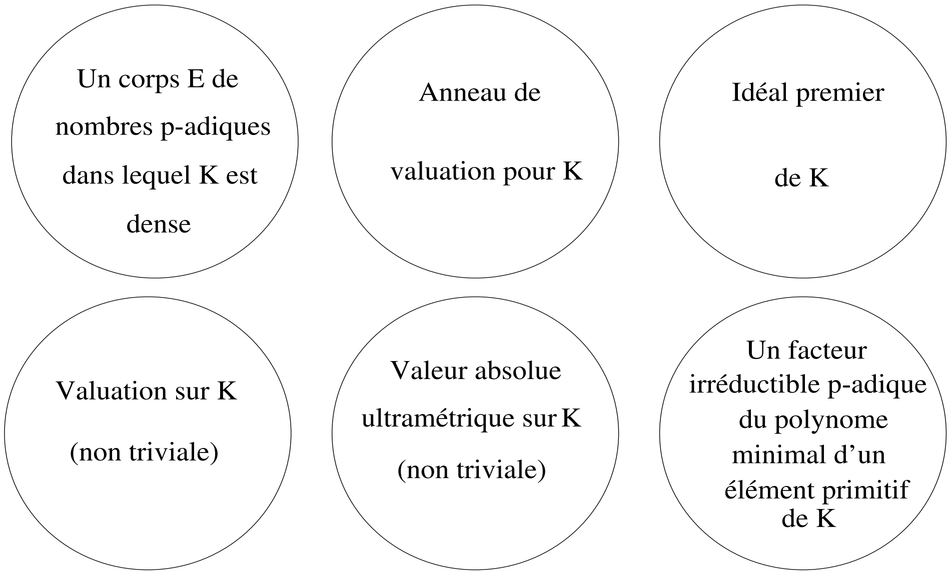
Pour finir, si on note $\mathfrak{P}$ l'unique idéal maximal de $\mathcal{O}_E$, alors $\mathfrak{p} = \mathfrak{P}\cap\mathcal{O}$ est un idéal premier de $\mathcal{O}$ qui contient p. En effet, comme $\mathbb{Z}_p \subset \mathcal{O}_E$ est une extension entière d'anneaux, $\mathfrak{P}\cap\mathbb{Z}_p$ est un premier **non nul** de $\mathbb{Z}_p$, donc $\mathfrak{P}\cap\mathbb{Z}_p = p\mathbb{Z}_p$ (l'anneau $\mathbb{Z}_p$ est local ; son unique idéal maximal est l'idéal $p\mathbb{Z}_p$). On vient donc d'associer à g, un facteur irréductible de f dans $\mathbb{Z}_p[X]$, un idéal premier de K au dessus de p, à savoir $\mathfrak{p}$.

Inversement, si $\mathfrak{p}$ est un premier de K au dessus de p, on veut lui faire correspondre un facteur irréductible de f dans $\mathbb{Z}_p[X]$. Pour cela, s'aidant du fait que $\mathcal{O}$ est un anneau de Dedekind, on construit une valeur absolue $|\ |$ sur K (intimement liée à l'idéal $\mathfrak{p}$), qui prolonge $|\ |_p$ la valeur absolue p-adique sur $\mathbb{Q}$. Alors le complété E de K pour $|\ |$ est à la fois une extension de K et de $\mathbb{Q}_p$. On montre (encore grâce à l'analyse) que E est de dimension finie sur $\mathbb{Q}_p$ en établissant l'égalité $E = \mathbb{Q}_p[\theta]$ où $\theta \in K$ entier sur $\mathbb{Z}$ est tel que $K = \mathbb{Q}[\theta]$. Considérons maintenant $g \in \mathbb{Z}_p[X]$ le polynôme minimal de θ sur $\mathbb{Q}_p$, alors g est bien un diviseur irréductible de f dans $\mathbb{Q}_p[X]$. On vient donc d'associer à $\mathfrak{p}$ idéal premier de K au dessus de p, un diviseur irréductible de f dans $\mathbb{Z}_p[X]$, ce que l'on voulait.

Cela étant, comme le lecteur a pu le remarquer, à plusieurs reprises, au cours de cette esquisse de preuve, on a eu besoin de résultats concernant les corps munis d'une valeur absolue (complets ou non pour cette dernière). Il m'a donc semblé intéressant de présenter une introduction à la théorie des valuations à travers la proposition 1. En effet cette dernière permet de réinvestir **dans un cadre concret** un bon nombre de résultats généraux de cette théorie.

I A propos de Localisation-Complétion-Globalisation

Nous allons dans cette section mettre en relation plusieurs objets. Plus précisément, étant donné K un corps de nombres, i.e. une extension finie de $\mathbb{Q}$, nous allons montrer l'équivalence entre les objets suivants :



I.1 Valuation

On considère K un corps (commutatif !). On appelle valuation réelle (c'est la structure du groupe totalement ordonné de $(\mathbb{R},+)$ que l'on retient ici, nous donnerons d'ailleurs ultérieurement une définition plus générale de la notion de valuation en utilisant à l'arrivée un groupe abélien totalement ordonné) sur K une application $v : K \to \mathbb{R} \cup \{\infty\}$ qui vérifie les trois axiomes suivants :

1. $v(xy) = v(x) + v(y) \quad \forall x, y \in K,$
2. $v(x+y) \geqslant \min\{v(x), v(y)\} \quad \forall x, y \in K,$
3. $v(x) = \infty \Leftrightarrow x = 0.$

Dès lors, grâce au premier axiome, on s'aperçoit que :

$$v(1) = 0, \qquad v(x^{-1}) = -v(x) \quad \forall x \in K \setminus \{0\} \qquad \text{et} \qquad v(x/y) = v(x) - v(y) \quad \forall x \in K,\ y \in K^*.$$

Quelques exemples :

• Pour un quelconque corps, la fonction qui s'annule en tout élément sauf en zéro (où elle prend la valeur ∞) est donc une valuation : c'est la valuation triviale. Elle ne présente que peu d'intérêt ; c'est pourquoi, dans tout ce qui suit, les valuations considérées seront implicitement supposées non triviales. Passons à des exemples simples (mais non triviaux !).

• On peut munir $\mathbb{Q}$ de la valuation p-adique v_p, où p est un premier de $\mathbb{Z}$. Pour $x \in \mathbb{Z}$, $v_p(x)$ désigne l'exposant du premier p dans la décomposition primaire de x. Cette fonction se prolonge, comme on le pense, au corps $\mathbb{Q}$. On obtient ainsi une valuation sur $\mathbb{Q}$.

De la même manière, si A est un anneau factoriel, alors pour tout irréductible $\pi \in A$, on peut construire une valuation sur le corps $\mathrm{Frac}(A)$ à partir de l'exposant de π.

• Considérons maintenant k un corps commutatif et $k(t)$ un corps de fractions rationnelles. Alors le sous-anneau $k[t]$ est principal ; ainsi, à tout irréductible $\pi \in k[t]$ est associé une valuation v_π sur $k(t)$ définie, comme précédemment, à partir de l'exposant dans la décomposition primaire. Par exemple, si $\pi = t$, alors on vérifie que pour toute fraction rationnelle $f/g \in k(t)$, on a :

$$v_t(f/g) = \mathrm{ordre}(f) - \mathrm{ordre}(g)$$

Sur $k(t)$, il existe une autre valuation couramment noté v_∞ et définie par :

$$v_\infty(f/g) = \deg(g) - \deg(f)$$

Nous verrons, d'ici peu, que ces valuations décrivent exactement l'ensemble des valuations sur $k(t)$ triviales sur k.

• Soit A un anneau de Dedekind dont on note K le corps des fractions (penser à un corps de nombres et son anneau d'entiers). A tout idéal premier $\mathfrak{p}$ de A (sous-entendu, une fois pour toutes, non nul), on associe l'application $v_{\mathfrak{p}}$ définie comme suit : si $x \in A$, $v_{\mathfrak{p}}(x)$ est l'exposant de l'idéal $\mathfrak{p}$ dans la factorisation en idéaux premiers de l'idéal $\langle x \rangle$. Encore une fois, on peut prolonger $v_{\mathfrak{p}}$ au corps K ; cela fournit une valuation sur ce dernier.

Considérons par exemple K un corps de nombres, et notons $\mathcal{O}$ son anneau d'entiers. Soit $\mathfrak{p}$ un premier de $\mathcal{O}$ et $v_{\mathfrak{p}}$ la valuation sur K qui lui est associé. Bien évidemment, $v_{\mathfrak{p}}$ induit, par restriction, une valuation sur $\mathbb{Q}$. C'est presque la valuation p-adique ; en effet, soit p le premier de $\mathbb{Z}$ que couvre $\mathfrak{p}$ i.e. $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. Alors si e est l'exposant de $\mathfrak{p}$ dans la factorisation de $\langle p \rangle$ en premiers de $\mathcal{O}$, on vérifie aisément que sur $\mathbb{Q}$, $v_p = v_{\mathfrak{p}}/e$. Autrement dit, à chaque premier $\mathfrak{p}$ de $\mathcal{O}$ au dessus de p est associé un prolongement de v_p au corps de nombres K. Il apparaît donc déjà un lien entre deux des différents objets cités en introduction.

De manière analogue, on montre que :

Proposition 2 *Soit A un anneau principal de corps des fractions K, L une extension finie et séparable de K et B la fermeture intégrale de A dans L (que l'on sait être un anneau de Dedekind). On considère π un premier de A ; à chaque premier $\mathfrak{p}$ de B au dessus de $\langle \pi \rangle$ est associé un prolongement de la valuation v_π (définie sur K) au corps L.*

Remarquons que mise à part la valuation triviale, toutes les valuations considérées vérifient $v(K^*) = \mathbb{Z}$ ou éventuellement $v(K^*) = \lambda\mathbb{Z}$ pour un certain λ de $\mathbb{R}^*$. Les valuations qui vérifient cette propriété sont dites **discrètes**. De manière générale, on dit qu'une valuation v est une **valuation discrète** si $v(K^*)$ est un sous-groupe discret de $\mathbb{R}$, donc de la forme $\lambda\mathbb{Z}$. Pour ce type de valuation, il existe donc $\pi \in K$ tel que $v(\pi)$ soit un générateur de $v(K^*)$. Un tel élément π est appelé **une uniformisante de** v. Ces éléments jouent un rôle important comme nous le constaterons dans la suite.

I.2 Anneau de valuation

I.2.1 Définition et premières propriétés

Nous allons maintenant introduire un des objets dont il est question dans l'introduction : les anneaux de valuation. Soit K un corps muni d'une valuation v, on vérifie aisément (grâce aux trois axiomes de départ) que l'ensemble :

$$V = \{x \in K,\ v(x) \geqslant 0\}$$

est un sous-anneau de K. On dit que V est **l'anneau de valuation pour** K **associé à** v. Par exemple, l'anneau de valuation pour $\mathbb{Q}$ associé à $v = v_p$ est le localisé de $\mathbb{Z}$ par l'idéal $\langle p \rangle$ que l'on note $\mathbb{Z}_{(p)}$. De même, si A est un anneau de Dedekind de corps des fractions K, alors pour tout premier $\mathfrak{p}$ de A, l'anneau de valuation pour K associé à $v_{\mathfrak{p}}$ est encore le localisé de A par $\mathfrak{p}$ noté $A_{\mathfrak{p}}$. Au passage, je rappelle l'une des caractérisations d'un anneau de Dedekind où il y est question d'anneaux de valuation :

Définition 1 *Soit A un anneau intègre, on dit que A est un anneau de Dedekind s'il est nœthérien et si pour tout idéal premier non nul $\mathfrak{p}$, le localisé de A par $\mathfrak{p}$, $A_{\mathfrak{p}}$, est un anneau de valuation discrète.*

Nous utiliserons cette caractérisation à plusieurs reprises dans la suite ; mais revenons, tout d'abord, à l'anneau V défini précédemment et remarquons que ce dernier vérifie :

Propriété 1 *Soit K un corps muni d'une valuation v, alors l'anneau de valuation pour K associé à V vérifie :*

$$x \in K \setminus V \quad \Longrightarrow \quad x^{-1} \in V.$$

Preuve — En effet, si $x \in K \setminus V$ alors $v(x) < 0$ donc $v(x^{-1}) = -v(x) > 0$, d'où $x^{-1} \in V$. □

En particulier, cela implique que le corps de fractions de V est K. De même, on montre facilement que V vérifie :

Propriété 2 *Avec les hypothèses de la proposition précédente, le corps des fractions de V est le corps K et l'ensemble des idéaux de V est totalement ordonné.*

Preuve — On s'est déjà aperçu du fait que le corps des fractions de V est K. On montre tout d'abord que l'ensemble des idéaux principaux est totalement ordonné. Soit x et y deux éléments non nuls de V. De deux choses l'une, ou bien $v(x/y) \geqslant 0$ ou bien $v(y/x) \geqslant 0$. Autrement dit, ou bien $x/y \in V$, ou bien $y/x \in V$. Par suite, ou bien y divise x (dans V) ou bien x divise y. Ainsi l'ensemble des idéaux principaux de V est bien totalement ordonné. Considérons maintenant I et J deux idéaux de V. Si $I \not\subset J$ et $J \not\subset I$, alors on peut trouver $x \in I \setminus J$ et $y \in J \setminus I$. Pour ces deux éléments, on a donc $\langle x \rangle \not\subset \langle y \rangle$ et $\langle y \rangle \not\subset \langle x \rangle$ ce qui contredit le premier point. $\square$

Les deux propriétés précédentes sont en fait équivalentes (c.f. l'annexe A), et définissent les anneaux de valuation pour K dans un cadre général où il n'est pas question de valuation. On peut vérifier que la donnée d'une valuation (à valeurs dans un groupe abélien totalement ordonné) sur un corps est équivalente à la donnée d'un anneau de valuation pour ce même corps. Nous ne nous étendrons pas plus sur la question ; introduisons plutôt :

$$\mathfrak{m}(V) = \{x \in K,\ v(x) > 0\}$$

c'est un idéal de V.

Remarque – Plus généralement, pour tout $\alpha \geqslant 0$, les ensembles $I_\alpha = \{x \in K,\ v(x) > \alpha\}$ et $I'_\alpha = \{x \in K,\ v(x) \geqslant \alpha\}$ sont des idéaux de l'anneau de valuation V pour K associé à v.

Mieux, on a en fait :

Proposition 3 *Soit K un corps muni d'une valuation v ; on note V l'anneau de valuation pour K associé à v alors,*

1. *l'anneau V est local d'idéal maximal $\mathfrak{m}(V)$.*
2. *on peut donner une propriété plus précise que la propriété 1 :*

$$x \in K \setminus V \quad \Longrightarrow \quad x^{-1} \in \mathfrak{m}(V).$$

3. *l'anneau V est intégralement clos.*

Preuve — Pour montrer que V est local, il suffit d'utiliser le fait que l'ensemble des idéaux de V est totalement ordonné (c.f. propriété 2). Cependant, on peut aussi remarquer que $\mathrm{U}(V) = \{x \in K,\ v(x) = 0\}$. En effet, si $x \in V$ vérifie $v(x) = 0$ alors $v(x^{-1}) = -v(x) = 0$, d'où $x^{-1} \in V$. Inversement, si x est inversible dans V alors $v(x)$ est à la fois positif et négatif, c'est à dire $v(x) = 0$. En conséquence $V \setminus \mathrm{U}(V) = \mathfrak{m}(V)$; le complémentaire dans V de l'ensemble de ses inversibles est par conséquent un idéal de V. Cela suffit pour montrer que V est un anneau local d'idéal maximal $\mathfrak{m}(V)$.

Ensuite il suffit de relire la preuve de la propriété 1 pour s'apercevoir que l'on y démontre ce que l'on veut.

Enfin, on considère $x \in K$ entier sur V qui vérifie une relation de dépendance intégrale du type : $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ (avec $a_i \in V$ bien sûr). Supposons $x \notin V$. Alors $x^{-1} \in \mathfrak{m}(V)$. Ainsi :

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \quad \overset{\times x^{-n}}{\Longrightarrow} \quad 1 + \frac{a_{n-1}}{x} + \cdots + \frac{a_0}{x^n} = 0,$$

donc $1 \in \mathfrak{m}(V)$, ce qui est impossible. $\square$

Enfin, si on suppose de plus que la valuation v est discrète, alors :

Proposition 4 *Soit K un corps muni d'une valuation discrète alors l'anneau de valuation V associé, que l'on sait être local, est de plus principal. L'anneau V est dit de valuation discrète.*

Preuve — Pour fixer les idées, on suppose que $v(K^*) = \mathbb{Z}$. Sinon, dans toute la suite, il suffit de remplacer 1 par un générateur positif de $v(K^*)$. Soit $\pi \in V$ tel que $v(\pi) = 1$. Alors pour tout $x \in V^*$,

$$v(x) = v(\pi^{v(x)}) \quad \text{i.e.} \quad v(x/\pi^{v(x)}) = 0.$$

Par conséquent, $x/\pi^{v(x)} \in \mathrm{U}(V)$. On vient donc de montrer que tout élément de V est associé dans V à une puissance de π. L'anneau V est donc principal (en plus d'être local). $\square$

L'élément π mis en avant dans la preuve précédente, n'est rien d'autre qu'une uniformisante de V au sens où nous l'avons déjà défini plus haut. Autrement dit, côté valuation discrète, une uniformisante est un élément dont la valuation engendre le groupe des valeurs de la valuation ; côté anneau de valuation discrète, une uniformisante est un générateur de l'(unique) idéal maximal (qui est principal).

I.2.2 Les anneaux de valuation pour un corps de nombres

Nous allons maintenant caractériser les anneaux de valuation pour un corps de nombres. Soit K un corps de nombres et V un anneau de valuation pour ce dernier ; dans toute la suite, on suppose que V est distinct de K. Remarquons tout d'abord qu'en tant que sous-anneau d'un corps de caractéristique zéro, V contient nécessairement $\mathbb{Z}$. Mieux, nous allons montrer que V contient en fait $\mathcal{O}$ l'anneau des entiers de K. Cela découle directement du lemme suivant :

Lemme 1 *Soit K un corps et A un sous-anneau de K. On considère V un anneau de valuation pour K* ***contenant*** *A ; alors V contient la clôture intégrale de A dans K.*

Preuve — Soit $x \in K$ entier sur A. Alors en particulier, comme $A \subset V$, il est entier sur V. Par conséquent, V étant intégralement clos, on a $x \in V$ d'où le résultat. □

Avant de caractériser de manière plus précise les anneaux de valuation d'un corps de nombres, j'ai besoin d'introduire une notion et de montrer quelques résultats.

Définition 2 *Soit A et B deux anneaux locaux dont on note $\mathfrak{m}$ et $\mathfrak{M}$ les idéaux maximaux respectifs. On dit que B domine A si et seulement si A est un sous-anneau de B et $\mathfrak{M} \cap A = \mathfrak{m}$.*

Proposition 5 *Soit K un corps et V un anneau de valuation pour K. Si $B \subset K$ est un anneau* ***local*** *qui domine V alors $V = B$.*

Preuve — Comme B domine V, $V \subset B$. Il suffit donc d'assurer l'inclusion inverse. On note $\mathfrak{m}(V)$ et $\mathfrak{m}(B)$ les idéaux maximaux respectifs de V et B. Soit $x \in K \setminus V$, alors $x^{-1} \in \mathfrak{m}(V)$. Mais par définition de la relation de domination, $\mathfrak{m}(V) = \mathfrak{m}(B) \cap V$. Par conséquent, $x^{-1} \in \mathfrak{m}(B)$ donc $x \notin B$, ce qu'il fallait montrer. □

Utilisons la proposition précédente pour montrer que :

Lemme 2 *Soit A un anneau de Dedekind (qui n'est pas un corps) de corps des fractions K et B un anneau* ***local*** *tel que $A \subset B \subsetneq K$. Notons $\mathfrak{m}$ l'idéal maximal de B, alors $\mathfrak{p} = A \cap \mathfrak{m}$ est un idéal premier non nul de A et l'anneau B n'est rien d'autre que le localisé $A_{\mathfrak{p}}$ de A par $\mathfrak{p}$.*

Preuve — Soit $x \in \mathfrak{m} \setminus \{0\}$ (cet élément existe car on a supposé que B n'est pas le corps K tout entier). Comme $\mathrm{Frac}(A) = K$, x se met sous la forme $x = a/b$ avec $a, b \in A \setminus \{0\}$. Par conséquent, $a = bx \in A \cap \mathfrak{m} \setminus \{0\}$. Ainsi, $\mathfrak{p} = A \cap \mathfrak{m}$ est bien un idéal premier non nul de A. De plus, $A \setminus \mathfrak{p} \subset B \setminus \mathfrak{m} = \mathrm{U}(B)$; ainsi, $A_{\mathfrak{p}} \subset B$. Pour conclure, il suffit de remarquer que $A_{\mathfrak{p}}$ étant un anneau de valuation (car A est de Dedekind, c.f. définition 1), comme B le domine, en vertu de la proposition 5, on a en fait l'égalité, i.e. $B = A_{\mathfrak{p}}$, ce que l'on voulait. □

Montrons de plus que :

Proposition 6 *Soit A un anneau de Dedekind (qui n'est pas un corps) de corps des fractions K. Alors les anneaux de valuation pour K contenant A et distincts de K sont exactement les localisés $A_{\mathfrak{p}}$ de A par les idéaux premiers de A.*

Preuve — Si $\mathfrak{p}$ est un idéal premier de A alors A étant de Dedekind, $A_{\mathfrak{p}}$ est un anneau de valuation (discrète). Réciproquement, si V est un anneau de valuation pour K contenant A, alors V étant en particulier local, c'est un $A_{\mathfrak{p}}$ en vertu du lemme précédent. □

Tout est prêt maintenant pour caractériser les anneaux de valuation pour un corps de nombres :

Théorème 1 *Soit K un corps de nombres, alors il y a une correspondance bi-univoque entre les idéaux premiers de K et les anneaux de valuation pour K. Plus précisément, si $\mathcal{O}$ désigne l'anneau des entiers de K et $\mathrm{Val}(K)$ l'ensemble des anneaux de valuation pour K, alors la correspondance précédente est donnée par :*

$$\begin{array}{ccc} \mathrm{Spec}(\mathcal{O}) & \longleftrightarrow & \mathrm{Val}(K) \\ \mathfrak{p} & \longmapsto & \mathcal{O}_{\mathfrak{p}} \\ \mathfrak{m}(V) \cap \mathcal{O} & \longleftarrow\!\shortmid & V \end{array}$$

Preuve — L'anneau des entiers de K, $\mathcal{O}$, étant de Dedekind, pour tout premier $\mathfrak{p}$ de $\mathcal{O}$, $\mathcal{O}_{\mathfrak{p}}$ est un anneau de valuation (discrète) pour K. Réciproquement, on considère V un anneau de valuation pour K alors ce dernier contient $\mathcal{O}$ comme nous avons pu le constater précédemment. Ainsi, $\mathcal{O}$ étant de Dedekind, nous pouvons appliquer la proposition précédente ; cela donne directement le résultat voulu. □

En particulier, les anneaux de valuation pour le corps de nombres $\mathbb{Q}$ sont donc les localisés de $\mathbb{Z}$ en ses premiers.

Dans le cadre des corps de nombres, tous les anneaux de valuation sont donc discrets.

En fait, le théorème précédent est un cas bien particulier d'un résultat plus général que nous rappellerons dans la section A. Dans ce dernier, les idéaux premiers et les idéaux maximaux ne jouent pas le même rôle. Ceci n'apparait pas ici car tous les anneaux manipulés sont de dimension 1 (i.e. tout idéal premier non nul est maximal). Cela sera, d'ailleurs, encore le cas dans la section qui suit :

I.2.3 Les anneaux de valuation pour un corps de fractions rationnelles

Soit k un corps commutatif et $k(t)$ un corps de fractions rationnelles. Intéressons nous aux anneaux de valuation pour le corps $k(t)$ et plus particulièrement à ceux qui contiennent k. On a le résultat classique suivant (c.f. (par exemple) [3], Chap 6, §1, n°4) :

Proposition 7 *Soit k un corps et $k(t)$ un corps de fractions rationnelles sur k. On considère V un anneau de valuation pour $k(t)$ contenant k (et distinct de $k(t)$) ; deux cas se présentent :*

1. *si $t \in V$ alors il existe un irréductible π de $k[t]$ tel que V soit le localisé de $k[t]$ par l'idéal $\langle \pi \rangle$;*
2. *sinon, V est le localisé de l'anneau $k[t^{-1}]$ par l'idéal $\langle t^{-1} \rangle$, c'est à dire :*

$$V = \{f/g \in k(t),\ \deg(f) \leqslant \deg(g)\}$$

Preuve — Le premier point découle encore directement de la proposition 6 ; en effet, si $t \in V$ alors comme V contient k par hypothèse, on a en fait $k[t] \subset V$.

Pour le deuxième point, on remarque que si $t \notin V$ alors (V étant un anneau de valuation) $t^{-1} \in V$ ce qui entraine que $k[t^{-1}] \subset V$; V est donc cette fois un localisé de $k[t^{-1}]$. L'anneau V ne peut être que le localisé de $k[t^{-1}]$ par l'idéal $\langle t^{-1} \rangle$ car nécessairement $t^{-1} \in \mathfrak{m}(V)$ (où $\mathfrak{m}(V)$ désigne l'idéal maximal de V). □

Côté valuation, nous venons de montrer que les seules valuations sur $k(t)$ triviales sur k sont les valuation v_π où π est un irréductible de $k[t]$ auquelles il convient d'ajouter la valuation v_∞ déjà définie. Ainsi, étant donné K une extension pure de degré de transcendance 1 de k, le choix d'un générateur de l'extension K/k permet de décrire toutes les valuations sur K triviales sur k. Nous utiliserons cette description ultérieurement (c.f. la section II.7)

I.3 Valeur absolue

Pour faire le lien avec la section suivante, nous allons introduire le langage des valeurs absolues. Il nous sera alors possible de réinvestir dans notre cadre des résultats classiques d'analyse. Nous en mesurerons par la suite de très nombreuses retombées purement algébriques. Mais n'anticipons pas plus et considérons K un corps muni d'une valuation v réelle, alors pour tout $0 < \xi < 1$, l'application :

$$x \longmapsto \begin{cases} \xi^{v(x)} & \text{si } x \neq 0 \\ 0 & \text{sinon} \end{cases}$$

est une valeur absolue **ultra-métrique** (on dit aussi **non archimédienne**) sur K, i.e. une application $|\ | : K \to \mathbb{R}_+$ qui vérifie les trois axiomes :

1. $|x| = 0 \iff x = 0$,
2. $|xy| = |x||y|$,
3. $|x + y| \leqslant \max\{|x|, |y|\}$.

Remarque – La définition précédente est très proche de la définiton usuelle de valeur absolue. Au lieu d'avoir la classique inégalité triangulaire, i.e. $|x + y| \leqslant |x| + |y|$ on exige ici la troisième propriété qui est plus forte d'où l'adjectif **ultra-métrique**. Le fait de travailler avec des valeurs absolues non archimédiennes est fondamental, car c'est grâce à cette propriété que l'analyse aura dans la suite des retombées algébriques.

Inversement si $|\ |$ est une valeur absolue réelle définie sur un corps K, alors $x \mapsto \log_\xi(|x|)$ est une valuation sur K.

Par exemple, dans le cadre des rationnels muni de la valuation p-adique, la valeur absolue p-adique $|\ |_p$ associée à v_p est définie par :

$$\forall x \in \mathbb{Q}, \quad |x|_p = p^{-v_p(x)}$$

(on choisit $\xi = 1/p$ pour des raisons que je ne développerai pas). De la même façon, à partir du prolongement v de v_p au corps de nombres K, on peut introduire un prolongement $|\ |$ de la valeur absolue p-adique $|\ |_p$ (intimement lié à un premier $\mathfrak{p}$ de K au dessus de p) :

$$\forall x \in K, \quad |x| = p^{-v(x)}.$$

On peut se demander l'utilité de ce "double langage". En fait, le langage "valeur absolue" présente l'énorme avantage de faire du corps K un espace métrique. En effet, dans le cas général, si un corps K est muni d'une valeur absolue $|\ |$ (ultra-métrique ou non), alors, $(K, |\ |)$ devient un espace métrique ; la distance d étant définie usuellement par : $d(x, y) = |x - y|$. On peut donc définir de manière naturelle toutes les notions métriques comme les suites de Cauchy ...

I.4 Le triangle LCG : Localisation-Complétion-Globalisation

Une fois n'est pas coutume, donnons un exemple d'application, ou plutôt une illustration du fameux triangle LCG (histoire de (peut-être ?) sensibiliser l'éventuel lecteur), avant de nous avoir donné les moyens de ces raisonnements. Intéressons nous à la propriété suivante : soient K et K' deux corps de nombres et p un premier de $\mathbb{Z}$; si p ne se ramifie ni dans K ni dans K', alors p ne se ramifie pas dans un compositum KK'. Une preuve possible de ce résultat consiste à localiser : soit $\mathfrak{P}$ un premier de KK' au dessus de p ; on introduit $(KK')_{\mathfrak{P}}$ le complété de KK' par rapport au premier $\mathfrak{P}$[2]. Cet idéal induit, par restriction, deux idéaux, $\mathfrak{p}$ et $\mathfrak{p}'$, de K et K' respectivement (tous deux au dessus de p évidemment). La "jolie" formule $(KK')_{\mathfrak{P}} = K_{\mathfrak{p}}K'_{\mathfrak{p}'}$ se révèle être la traduction d'un résultat véridique, à savoir : le complété du compositum de deux extensions **finies** est le compositum des complétés[3]. Comme le premier p ne se ramifie ni dans K ni dans K', les extensions, $K_{\mathfrak{p}}/\mathbb{Q}_p$ et $K'_{\mathfrak{p}'}/\mathbb{Q}_p$ sont toutes deux **non ramifiées**. Dès lors, et c'est là que la magie de la localisation-complétion opère, il en est de même de l'extension $(KK')_{\mathfrak{P}}/\mathbb{Q}_p$ car le compositum de deux extensions non ramifiées de **corps locaux** (c.f. Définition 3) est encore non ramifié (résultat classique de la théorie des corps locaux s'il en est). En "globalisant", l'information "locale" que nous venons d'obtenir, on montre que l'exposant de l'idéal $\mathfrak{P}$ dans la factorisation de p dans le corps KK' est 1. Réitérant ce raisonnement pour tous les premiers de KK' au dessus de p, on montre[4] bien que ce dernier ne se ramifie pas dans le compositum KK'.

En particulier, nous venons d'établir la propriété suivante : un premier p est non ramifié dans un corps de nombres K si et seulement s'il ne l'est dans pas dans sa clôture galoisienne.

La suite de cette section est constituée de rappels de résultats généraux redémontrés en partie. Il ne s'agit évidemment pas de rivaliser avec les grands classiques[5], mais plutôt de donner un peu (semblant ?) de cohésion à ce document.

I.4.1 Complétion

Entre autres questions, on peut par exemple se poser le problème de savoir si un corps K muni d'une valeur absolue $|\ |$ fait de l'espace métrique $(K, |\ |)$ un espace complet ou non. Bien évidemment, ce n'est pas toujours le cas ; en revanche, on peut établir que :

Proposition 8 *Soit $(K, |\ |)$ un corps muni d'une valeur absolue $|\ |$. Il existe un sur-corps $\widehat{K}$ de K muni d'une valeur absolue $|\ |$ prolongeant celle de K et complet pour $|\ |$ tel que K soit dense dans $\widehat{K}$ (pour la métrique associée à $|\ |$ bien sûr). De plus, ce sur-corps est unique à un K-isomorphisme près.*

Preuve — On construit le complété de K pour $|\ |$ comme on construit $\mathbb{R}$ à partir des suites de Cauchy de $\mathbb{Q}$ pour la valeur absolue usuelle. Les suites de Cauchy forment un anneau A dans lequel K s'injecte.

---

[2] On complète en fait par rapport à la valuation $|\ |_{\mathfrak{P}}$; nous y reviendrons dans la section I.4.1.

[3] Les hypothèses restent bien sûr à préciser, mais en fait cela cache un phénomène bien plus général englobant largement notre cadre des corps de nombres p-adiques. De plus, la preuve du résultat est élémentaire comme nous le verrons dans la suite (c.f. section I.4.4).

[4] On voit ici un autre aspect de la puissance des raisonnements "localisant" : ils permettent de se polariser sur un seul premier.

[5] Pour ne citer que lui, J-P.Serre dans la première partie de son ouvrage "Corps Locaux" ([21]), intitulée "Généralités" comme par hasard, frappe très vite et très fort.

L'idéal I formé des suites qui tendent vers zéro est maximal dans A. Le complété de K pour $|\ |$ est le quotient A/I. Serge Lang dans [14] rappelle ce procédé de construction dans la preuve de la proposition 2.1 du Chap XII, § 2. □

Par continuité, la valeur absolue du corps de base est ultra-métrique si et seulement si le prolongement du complété l'est. De plus, si la valeur absolue $|\ |$ sur K est non archimédienne alors l'ensemble des valeurs prises par $|\ |$ sur K est le même que celui sur le complété. En effet, soit $x \in \widehat{K}$; par densité, il existe $y \in K$ tel que $|x - y| < |x|$, de telle sorte que $|x| = |y|$. En conséquence, si la valeur absolue $|\ |$ provient d'une valuation discrète, il est est de même de son prolongement au complété.

Définition 3 *Un corps muni d'une valeur absolue provenant d'une valuation discrète, qui plus est complet, est communément appelé* ***corps local****.*

Le premier complété rencontré par un étudiant en mathématiques est bien entendu le corps des nombres réels, $\mathbb{R}$, qui est le complété de $\mathbb{Q}$ pour la valeur absolue usuelle. Mais on peut aussi compléter $\mathbb{Q}$ pour la valeur absolue p-adique $|\ |_p$; on obtient alors $\mathbb{Q}_p$ le corps des nombres p-adiques. L'anneau de valuation pour $\mathbb{Q}_p$ associé à $|\ |_p$ est l'anneau des entiers p-adiques que l'on note $\mathbb{Z}_p$. L'élément p reste extrémal dans $\mathbb{Z}_p$.

Allons encore un peu plus loin, et considérons K un corps de nombres. On sait qu'à chaque premier $\mathfrak{p}$ de K est associé un prolongement $|\ |$ à K de la valeur absolue p-adique (c.f. proposition 2). On peut bien entendu compléter K pour cette valeur absolue. Notons $K_{\mathfrak{p}}$ le sur-corps de K obtenu par ce procédé. En résumé :

$$\overbrace{\mathbb{Q} \qquad\qquad \mathbb{Q}_p}^{\text{complétion}} \qquad\qquad \overbrace{\mathbb{Q} \qquad\quad K}^{\text{alg.}} \qquad\qquad \overbrace{K \qquad\qquad K_{\mathfrak{p}}}^{\text{complétion}}.$$

Dans le cadre des corps de fractions rationnelles, si on munit $k[t]$ de la valuation associée au premier t (c'est à dire, je le rappelle, l'ordre d'un polynôme) et que l'on prolonge cette dernière à $k(t)$, en complétant, on obtient le corps $k((t))$ dont l'anneau est celui des séries formelles, i.e. $k[[t]]$.

Remarquons que les corps $\mathbb{Q}_p$, $K_{\mathfrak{p}}$ $k((t))$, sont complets chacun pour une valeur absolue provenant de valuations discrètes. Ce sont donc des corps locaux.

I.4.2 Unicité du prolongement d'une valeur absolue ultra-métrique complète

Nous énonçons ici l'un des théorèmes fondamentaux de la théorie des corps ultra-métriques complets (i.e. complets pour une valeur absolue ultra-métrique). Il s'agit du prolongement de la valeur absolue aux extensions finies. En fait, deux énoncés seront donnés, l'un général et un autre (plus précis) orienté corps locaux.

Le résultat général :

Théorème 2 *Soit $(K, |\ |)$ un corps ultra-métrique complet. La valeur absolue $|\ |$ se prolonge de manière unique à toute extension L* ***de degré fini*** *de K.*

Nous ne donnerons pas la démonstration de ce résultat dans toute sa généralité. Cependant, intéressons nous aux trames des différentes preuves que l'on peut faire de ce théorème. Tout d'abord, on peut montrer l'unicité par un raisonnement purement analytique, après avoir établi le lemme :

Lemme 3 *Soit K un corps muni de $|\ |_1$, $|\ |_2$, deux valeurs absolues sur K. Alors sont équivalentes :*

1. *il existe $\alpha,\ \beta \in \mathbb{R}_+^*$ tels que :*
$$\alpha|x|_1 \leqslant |x|_2 \leqslant \beta|x|_1 \quad \forall x \in K$$
2. *il existe $\gamma \in \mathbb{R}_+^*$ tel que $|\ |_1 = |\ |_2^{\gamma}$*

Preuve — Pour la preuve de ce résultat, je renvoie par exemple à [16] théorème 1.7 du Chap 12 §1. □

En particulier, considérons K un corps muni d'une valeur absolue $|\ |$ et L un sur-corps de K. Tout prolongement de la valeur absolue $|\ |$ au corps L fait de ce dernier un K-espace vectoriel normé. De plus, si $|\ |_1$ et $|\ |_2$ sont deux prolongements de $|\ |$ à L alors, pour que ces deux prolongements soient équivalents **au sens des normes**, il faut et il suffit que l'un soit une puissance de l'autre. Nous allons maintenant utiliser cette remarque pour montrer que :

Preuve de l'unicité (dans l'énoncé du théorème 2) — Supposons qu'il existe $|\ |_1$ et $|\ |_2$ deux valeurs absolues sur L qui prolongent la valeur absolue $|\ |$ de K. Alors $|\ |_1$ et $|\ |_2$ font de L un K-espace vectoriel normé de dimension finie. Or K étant complet pour $|\ |$, d'après le résultat classique d'analyse déja utilisé précédemment, $|\ |_1$ et $|\ |_2$ sont équivalentes (au sens des normes). Par suite, d'après le lemme 3, il existe un réel positif γ tel que : $|\ |_1 = |\ |_2^{\gamma}$. Mais comme $|\ |_1$ et $|\ |_2$ sont égales sur K, nécessairement $\gamma = 1$ d'où l'unicité. □

Cela étant, on distingue plusieurs méthodes dans la littérature pour établir l'existence d'un prolongement :
• Une première idée consiste à utiliser les théorèmes généraux de prolongements de valuations sur lesquels nous reviendrons dans l'annexe A (Note : l'hypothèse "complet" n'est pas utilisée pour montrer l'existence).
• Une stratégie très classique, part de l'expression, a priori, de l'unique prolongement :

$$\forall x \in L,\ |x|_L = |\,\mathrm{N}_{L/K}(x)|_K^{1/n} \quad \text{avec } n = [L:K] \tag{1}$$

On est alors ramené à montrer que cette formule définit bien une valeur absolue (ultra-métrique) sur L prolongeant, $|\ |_K$, la valeur absolue définie sur K. Le seul point qui pose problème est de vérifier que l'on a bien $|x+y|_L \leqslant \max\{|x|_L, |y|_L\}$ pour tous x et y de L. Cela peut se faire grâce au lemme de Hensel sur lequel nous reviendrons longuement dans la section IV (c.f. [16], Chap 14, §2, Théorème 2.1).

Remarque – Si la deuxième stratégie n'a pas été adoptée, il est tout de même intéressant de vérifier que l'unique prolongement, $|\ |_L$ peut s'exprimer sous la forme (1). Fixons Ω une clôture algébrique de L et considérons $x \in L$; on sait que la norme de ce dernier sur K se met sous la forme :

$$N_{L/K}(x) = y_1 \cdots y_n$$

où chaque $y_i \in \Omega$ est un conjugué de x sur K ; autrement dit, pour chaque $i \in [1..n]$, il existe $\sigma_i \in \mathrm{Hom}_K(L,\Omega)$ tel que $y_i = \sigma(x)$. Par ailleurs, compte tenu de l'unicité du prolongement de la valeur absolue $|\ |_L$ à toute extension algébrique finie de L, par recollement, cela donne un unique prolongement de $|\ |_L$ à Ω tout entier ; notons le $|\ |$. Etant donné $\sigma \in \mathrm{Hom}_K(L,\Omega)$, l'application $|\ | \circ \sigma$ définit un prolongement de $|\ |_K$ à L. Par unicité, on a donc :

$$\forall \sigma \in \mathrm{Hom}_K(L,\Omega),\ \forall x \in L \qquad |\sigma(x)| = |x|_L$$

Cette égalité est en particulier v'érifiée pour les n K-homomorphismes du début de cette remarque ; ainsi :

$$|\,\mathrm{N}_{L/K}(x)|_K = |\sigma_1(x)\cdots\sigma_n(x)| = |x|_L^n,$$

d'où la formule du départ. Il est intéressant de noter qu'aucune hypothèse sur la séparabilité des extensions n'a été nécessaire.

Dans le cadre des corps locaux :

Dans le cadre des **corps locaux**, on peut donner un énoncé encore plus précis. Ce dernier figure bien sûr dans [21] (Chap II, § 2, Proposition 3) :

Proposition 9 *Soit K un **corps local** dont on note A l'anneau de valuation. On considère L une extension **finie** de K ; alors L est un corps local dont l'anneau de valuation n'est rien d'autre que la fermeture intégrale B de A dans L. L'anneau B est donc un anneau de valuation discrète (i.e. local principal et distinct de son corps des fractions) ; il est de surcroît un A-module libre de rang égal à $[L:K]$.*

De plus, si on note $\mathfrak{m}$ et $\mathfrak{M}$ les idéaux maximaux respectifs des anneaux A et B, alors,

$$\mathfrak{m}B = \mathfrak{M}^e, \quad \textit{et} \quad [L:K] = ef \quad \textit{avec} \quad f = \dim_{A/\mathfrak{m}} B/\mathfrak{M}.$$

Esquisse de preuve : — On commence par montrer l'existence du prolongement de la valeur absolue $|\ |$ de K à toute extension **séparable** et finie de K. Si l'extension L/K est séparable, cela découle directement de la proposition 2 car le corps K étant local, l'anneau A est principal. Le fait que B soit un A-module de type fini est aussi une conséquence directe de la séparabilité (B est de plus un anneau de Dedekind). De l'unicité du prolongement préalablement prouvée, on déduit le caractère local de l'anneau B ce qui entraîne le fait que B soit de valuation discrète (Dedekind + Local = de Valuation Discrète !). En effet, considérons deux idéaux maximaux distincts de B, $\mathfrak{M}_1$ et $\mathfrak{M}_2$ au dessus de $\mathfrak{m}$ (l'idéal maximal de A) alors les deux valeurs absolues $|\ |_1$ et $|\ |_2$ respectivement associées, prolongent la valeur absolue $|\ |$ de K. Ces dernières sont nécessairement **distinctes** car $\mathfrak{M}_1$ et $\mathfrak{M}_2$ étant comaximaux, on peut trouver $x \in B$ tel que $x \in \mathfrak{M}_1$ mais $x \notin \mathfrak{M}_2$ de telle sorte que $|x|_1 \neq |x|_2$. Ceci achève la preuve de la proposition dans le cas où l'extension L/K est séparable ; en effet les dernières propriétés ne sont qu'une retranscription des résultats classiques concernant les anneaux de Dedekind.

Ensuite, suivant Serre (loc. cit.), je cite : "une fois ce cas traité, un argument de "dévissage" évident permet de se ramener au cas où L/K est radicielle"... □

Remarque – Ici, je considère acquise la relation $n = \sum e_i f_i$. Cependant, une des démonstrations de cette relation consiste à l'établir dans le cadre précédent puis à la "globaliser" aux anneaux de Dedekind. Cette démarche est celle suivie par Borevitch et Chafarevitch dans la section "Degrés résiduels" du Chap III, §5 de [2].

En particulier, dans le cadre des corps de nombres p-adiques, nous avons le résultat suivant :

Proposition 10 *Soit E un corps de nombres p-adiques (i.e. une extension finie de $\mathbb{Q}_p$). La fermeture intégrale, $\mathcal{O}_E$, de $\mathbb{Z}_p$ dans E est un anneau de valuation discrète ; de plus, si on note $\mathfrak{P}$ son (unique) idéal maximal, on a :*

$$p\mathcal{O}_E = \mathfrak{P}^e, \quad \textit{et} \quad [E : \mathbb{Q}_p] = ef \quad \textit{avec} \quad f = \dim_{\mathbb{F}_p} \mathcal{O}_E/\mathfrak{P}.$$

I.4.3 La complétion ne modifie pas les corps résiduels

Commençons par illustrer le titre de cette section à l'aide d'un exemple significatif : on considère $k((t))$ le corps des fractions de l'anneau des séries entières, $k[[t]]$. Ce corps est le complété du corps des fractions rationnelles, $k(t)$ pour la valuation v_t associée au premier t de $k[t]$. Alors il est clair que $k[t]$ l'anneau de valuation pour $k(t)$ associé à v_t est dense dans $k[[t]]$ l'anneau de valuation pour $k((t))$ associé à v_t. De plus, on a un isomorphisme canonique des corps résiduels :

$$k[t]/tk[t] \simeq k[[t]]/tk[[t]] \simeq k$$

En fait, plus généralement, on a :

Proposition 11 *Soit L un corps muni d'une valeur absolue $|\ |$ **ultramétrique** et K un sous-corps de L dense dans L. On considère V_L l'anneau de valuation de L associé à $|\ |$ et $\mathfrak{m}_L$ son idéal maximal. Alors, $V_K = V_L \cap K$ l'anneau de valuation de $|\ |_{|K}$ est dense dans V_L et a pour idéal maximal $\mathfrak{m}_K = \mathfrak{m}_L \cap V_K$; de plus, on a :*

$$\mathfrak{m}_K V_L = \mathfrak{m}_L \quad \textit{et} \quad V_K/\mathfrak{m}_K \simeq V_L/\mathfrak{m}_L.$$

Preuve — Tout repose sur la remarque suivante : comme K est dense dans L, pour tout $x \in L$, il existe $y \in K$ tel que $|y - x|$ soit aussi petit que l'on veut. En particulier, pour $x \in L \setminus \{0\}$, on peut trouver $y \in K$ tel que $|y - x| < |x|$. Mais alors en écrivant $y = x + (y - x)$, on obtient $|x| = |y|$ car $|\ |$ est **ultramétrique**. Plus précisément, si $\mathcal{B} = \mathcal{B}(0, r)$ est la boule de L (ouverte ou fermée, ça n'a pas d'importance ici) centrée en 0 et de rayon r, alors pour tout $x \in \mathcal{B} \setminus \{0\}$ et tout $\varepsilon \in \mathbb{R}_+^*$, il existe $y \in \mathcal{B} \cap K$ tel que $|x| = |y|$ et $|x - y| < \varepsilon$. Il suffit en effet de considérer $y \in K$ tel que $|x - y| < \min\{r, |x|, \varepsilon\}$.

Par définition de l'anneau de valuation associé à une valeur absolue ultramétrique, on a évidemment $V_K = V_L \cap K$ et $\mathfrak{m}_K = \mathfrak{m}_L \cap K$

• Montrons que V_K est dense dans V_L. Soit $x \in V_L$, il faut établir que pour tout $\varepsilon \in \mathbb{R}_+^*$, il existe $y \in V_K$ tel que $|x - y| < \varepsilon$. Comme V_L n'est rien d'autre que la boule (fermée) de L centrée en 0 et de rayon 1, il suffit d'appliquer la remarque précédente à $\mathcal{B}(0, 1) = V_L$ pour conclure.

• De même, pour $x \in V_L \setminus \{0\}$, si on considère $y \in V_K$ tel que $|x - y| < 1$ c'est à dire $x - y \in \mathfrak{m}_L$ ou encore $x \equiv y \mod \mathfrak{m}_L$ alors on établit la surjectivité de l'injection $V_K/\mathfrak{m}_K \to V_L/\mathfrak{m}_L$ (c'est une injection car $\mathfrak{m}_L \cap V_K = \mathfrak{m}_K$) d'où l'isomorphisme avancé.

• Enfin, pour $x \in \mathfrak{m}_L \setminus \{0\}$, si y est choisi dans $\mathfrak{m}_K$ pour vérifier $|y| = |x|$ (ce qui est possible car $\mathfrak{m}_L$ est la boule, ouverte cette fois, centrée en 0 et de rayon 1), alors l'écriture $x = y(xy^{-1})$ montre que $\mathfrak{m}_L \subset \mathfrak{m}_K V_L$ car $|xy^{-1}| = 1$ donc $xy^{-1} \in V_L$. La proposition est donc établie. □

Proposition 12 *Soit K un corps muni d'une valeur absolue $|\ |$ ultramétrique, V l'anneau de valuation associé à $|\ |$ et $\mathfrak{m}$ l'idéal maximal de V. Soit $\widehat{K}$ le complété de K pour $|\ |$, on note encore $|\ |$ le prolongement de $|\ |$ à $\widehat{K}$. Considérons $\widehat{V}$ l'anneau de valuation de $\widehat{K}$ associé à $|\ |$ et $\widehat{\mathfrak{m}}$ son idéal maximal. Alors $V = \widehat{V} \cap K$ et est dense dans $\widehat{V}$; de même, $\mathfrak{m} = \widehat{\mathfrak{m}} \cap V$ est dense dans $\widehat{\mathfrak{m}}$. On a de plus :*

$$\mathfrak{m}\widehat{V} = \widehat{\mathfrak{m}} \quad \textit{et} \quad V/\mathfrak{m} \simeq \widehat{V}/\widehat{\mathfrak{m}}.$$

Enfin, $|\ |$ prend les mêmes valeurs sur K et $\widehat{K}$.

Preuve — Comme K est dense dans $\widehat{K}$ on est exactement dans la situation de la proposition précédente car par continuité, $|\ |$ définie sur $\widehat{K}$ est ultramétrique elle aussi. □

Il nous reste désormais à assurer "une bascule" entre les propriétés d'un corps valué et de son complété ; par exemple, il est crutial, pour la suite, de mettre en évidence un lien entre un corps de nombres K et l'un des complétés $K_\mathfrak{p}$ évoqués ci-avant. En fait, il s'agit d'assurer le côté **globalisation** du triangle LCG.

I.4.4 Extension et complétion

Nous allons maintenant étudier de plus près l'extension $\mathbb{Q}_p \subset K_{\mathfrak{p}}$:

Proposition 13 *Soit L un corps muni d'une valeur absolue $|\ |$ et K un sous-corps de L tel que l'extension $K \subset L$ soit de degré fini. Alors $\widehat{L}$ contient $\widehat{K}$ le complété de K pour $|\ |_{|K}$; de plus $\widehat{L}$ est une extension de $\widehat{K}$ de degré fini et on a l'inégalité :*

$$[\widehat{L} : \widehat{K}] \leqslant [L : K].$$

Pour établir la proposition 13, nous allons utiliser des résultats classiques d'analyse concernant les espaces vectoriels sur les corps complets. Soit $(K, |\ |)$ un corps muni d'une valeur absolue et complet pour cette dernière, les trois propriétés suivantes sont connues :

1. Si E est un K-espace vectoriel de dimension finie alors toutes les normes sur E sont équivalentes.
2. Ce même espace vectoriel, E, normé par n'importe quelle norme est complet.
3. Si E (toujours supposé de dimension finie) est inclus dans F un autre K-espace vectoriel normé (mais non nécessairement de dimension finie), alors E est fermé dans F.

Les deux derniers résultats découlent assez directement du premier. Ce dernier est ultra classique pour $K = \mathbb{R}$ ou $\mathbb{C}$. On en trouve la preuve dans tous les livres de premier cycle. En général, un argument de locale compacité est invoqué. Pourtant cette propriété n'est pas nécessaire et seul le caractère complet du corps de base est utile. Pour une preuve n'utilisant que la complétude, je renvoie le lecteur aux ouvrages suivants : [14], Chap XII §2, Proposition 2.2, [6] Chap II §8 ou encore [16], Lemme 2.2 p. 206.

Preuve de la proposition 13 : — Le complété étant unique (à isomorphisme près), on a nécessairement $\widehat{K} \subset \widehat{L}$. Pour le reste de la proposition, on introduit $e_1, \ldots, e_n$ une K-base de L. Alors on a les inclusions $L \subset \widehat{K}e_1 + \cdots + \widehat{K}e_n \subset \widehat{L}$; d'où par densité :

$$\overline{\widehat{K}e_1 + \cdots + \widehat{K}e_n} = \widehat{L}$$

Pour conclure, il suffit maintenant de remarquer que $\widehat{K}e_1 + \cdots + \widehat{K}e_n$ est un sous $\widehat{K}$-espace vectoriel de dimension finie du $\widehat{K}$-espace vectoriel normé $\widehat{L}$. Par suite, en vertu du dernier résultat rappelé plus haut, le sous-ensemble $\widehat{K}e_1 + \cdots + \widehat{K}e_n$ est fermé dans $\widehat{L}$ d'où l'égalité $\widehat{K}e_1 + \cdots + \widehat{K}e_n = \widehat{L}$. Ceci montre bien que l'extension $\widehat{K} \subset \widehat{L}$ est finie et de degré inférieur ou égal à $[L : K]$. □

Il est bon de garder en tête l'esprit de la démonstration précédente. Plus précisément, on peut retenir que :

$$L = \sum_{i=1}^{n} Ke_i \qquad \Longrightarrow \qquad \widehat{L} = \sum_{i=1}^{n} \widehat{K}e_i$$

où L est bien sûr un corps muni d'une valeur absolue. En particulier, étant donnés $x_1, \ldots, x_n$ n éléments **algébriques** sur K, on a :

$$L = K(x_1, \ldots, x_n) \qquad \Longrightarrow \qquad \widehat{L} = \widehat{K}(x_1, \ldots, x_n)$$

En conséquence, si L/K et M/K sont deux K-extensions **finies** (toutes deux munies d'une valeur absolue ayant même restriction à K), alors, un "gros" corps contenant tout ce petit monde étant fixé, "le" compositum des complétés est "le" complété des compositums, c'est-à-dire en bref :

$$\widehat{LM} = \widehat{L}\widehat{M} \ ;$$

en effet, il suffit d'écrire $L = K(x_1, \ldots, x_n)$ et $M = K(y_1, \ldots, y_m)$ (où les x_i et les y_j sont algébriques sur K) alors $LM = K((x_i y_j)_{i,j})$ et par suite :

$$\widehat{LM} = \widehat{K}((x_i y_j)_{i,j}) = \widehat{K}(x_1, \ldots, x_n)\widehat{K}(y_1, \ldots, y_m) = \widehat{L}\widehat{M}$$

Tout est prêt désormais pour établir la correspondance :

I.4.5 Correspondance idéaux premiers de K et corps p-adiques dans lesquels K est dense

Revenons aux corps $\mathbb{Q}_p$ et $K_\mathfrak{p}$ introduits précédemment. Je rappelle que K est un corps de nombres (il joue le rôle du corps L de la proposition) que l'on munit du prolongement de la valuation p-adique $|\ |_p$ associé à un certain premier $\mathfrak{p}$ de K au dessus de p. Avec les notations précédentes, nous venons donc de montrer que le complété $K_\mathfrak{p}$ de K contient celui de $\mathbb{Q}$ i.e. $\mathbb{Q}_p$. De plus, l'extension $\mathbb{Q}_p \subset K_\mathfrak{p}$ est finie et on a l'inégalité :

$$[K_\mathfrak{p} : \mathbb{Q}_p] \leqslant [K : \mathbb{Q}].$$

Nous verrons par la suite que le degré $[K_\mathfrak{p} : \mathbb{Q}_p]$ "mesure" une quantité bien précise. Nous pouvons d'ores et déjà mettre en relation deux nouveaux objets du début de cette section, à savoir les idéaux premiers de K et les corps de nombres p-adiques dans lesquels K est dense. En effet, dans la démarche rappelée ci-avant, nous sommes partis d'un premier $\mathfrak{p}$ de K et nous avons "construit" $K_\mathfrak{p}$ un corps de nombres p-adiques (où p est l'entier tel que $\langle p\rangle = \mathfrak{p} \cap \mathbb{Z}$), dans lequel K est dense (par définition du complété). Réciproquement, considérons E un corps de nombres p-adiques dans lequel K est dense ; notons $\mathcal{O}$ l'anneau des entiers de K et $\mathcal{O}_E$ la fermeture intégrale de $\mathbb{Z}_p$ dans E. Alors on a évidemment $\mathcal{O} \subset \mathcal{O}_E$ et si $\mathfrak{P}$ est un premier de $\mathcal{O}_E$ au dessus de p, $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}$ est un idéal premier non nul de K (car contenant p). Nous pourrions nous en tenir là ; cependant, il est possible d'énoncer un résultat bien plus précis (noter par exemple que dans la réciproque précédente, la densité de K dans E n'a été, pour l'instant, d'aucune utilité). Nous sommes désormais en mesure de donner un résultat assez précis :

Proposition 14 *Il y a une correspondance bi-univoque entre les idéaux premiers de K au dessus de p et les corps de nombres p-adiques dans lesquels K est dense. Notons $\mathrm{Spec}_p(K)$ l'ensemble des premiers de K au dessus de p, $\mathrm{Ext}_{\mathbb{Q}_p}(K)$ l'ensemble des extensions de $\mathbb{Q}_p$ dans lesquelles K est dense, puis pour $E \in \mathrm{Ext}_{\mathbb{Q}_p}(K)$, $\mathfrak{P}_E$ l'(unique) idéal maximal de E. Alors la correspondance précédente est donnée par :*

$$\begin{array}{ccc} \mathrm{Spec}_p(K) & \longleftrightarrow & \mathrm{Ext}_{\mathbb{Q}_p}(K) \\ \mathfrak{p} & \longmapsto & K_\mathfrak{p} \\ \mathfrak{P}_E \cap K & \longleftarrow\!\shortmid & E \end{array}$$

De plus, si on appelle $\mathcal{O}$ l'anneau des entiers de K, $\mathcal{O}'$ celui de $K_\mathfrak{p}$ (i.e. la clôture intégrale de $\mathbb{Z}_p$ dans $K_\mathfrak{p}$) et $\mathfrak{P}$ l'(unique) idéal maximal de $\mathcal{O}'$, alors :

1. *le premier $\mathfrak{p}$ de K reste premier dans $K_\mathfrak{p}$, i.e. $\mathfrak{p}\mathcal{O}' = \mathfrak{P}$;*
2. *les corps résiduels sont isomorphes, i.e. $\mathcal{O}/\mathfrak{p} \simeq \mathcal{O}'/\mathfrak{P}$, de dimension commune sur $\mathbb{F}_p$ égale à $f_\mathfrak{p}$, le degré résiduel du premier $\mathfrak{p}$;*
3. *les indices de ramification de p par rapport à $\mathfrak{p}$ (dans K) et par rapport à $\mathfrak{P}$ (dans $K_\mathfrak{p}$) sont les mêmes ; autrement dit $p\mathcal{O}' = \mathfrak{P}^{e_\mathfrak{p}}$;*
4. *l'extension $\mathbb{Q}_p \subset K_\mathfrak{p}$ est de degré $e_\mathfrak{p} f_\mathfrak{p}$.*

Preuve — On sait, d'après le corollaire 9, que l'anneau $\mathcal{O}'$ est local. Cela nous a permis dans l'énoncé de la proposition précédente de parler de l'unique idéal maximal de $\mathcal{O}'$. Cela étant, tout est prêt pour établir la proposition maintenant. Il suffit en fait de remarquer que les corps K et $K_\mathfrak{p}$ vérifient les hypothèses de la proposition 12. Apparaît alors l'anneau $\mathcal{O}_\mathfrak{p} = \mathcal{O}' \cap K$ localisé de $\mathcal{O}$ par $\mathfrak{p}$; en effet, en vertu du théorème 1, l'anneau de valuation pour K associé au prolongement à K de la valeur absolue p-adique n'est rien d'autre que $\mathcal{O}_\mathfrak{p}$. Toutes les propriétés énoncées en remplaçant $\mathcal{O}$ par $\mathcal{O}_\mathfrak{p}$ découlent alors directement de la proposition 12. Pour revenir à $\mathcal{O}$ on utilise, entre autres, le fait que $\mathfrak{p}$ premier de $\mathcal{O}$ reste premier dans $\mathcal{O}_\mathfrak{p}$ et que les corps résiduels sont égaux ... □

Remarque – Bien que la proposition précédente ait été énoncée dans le cadre des corps de nombres, on peut donner un résultat analogue avec comme corps de base, un corps muni d'une valuation **discrète** (c.f. [21] (évidemment !), Chap II, §3, théorème 1).

Plus légèrement, on peut retenir de ce qui précède l'idée suivante : la complétion permet de polariser l'étude sur un seul idéal premier au dessus de p. Les autres sont "chassés" et le premier mis en avant a le même comportement "ici" et "dans le complété".

A l'issue de tout cela, si on souhaite ne garder que l'essentiel de l'information, on peut retenir le refrain :

Proposition 15 *Il y a une correspondance bi-univoque entre les idéaux premiers d'un corps de nombres K au dessus d'un premier p de $\mathbb{Z}$ et les extensions de $\mathbb{Q}_p$ de degré fini dans lesquelles K est dense.*

I.4.6 Retour aux polynômes

Seul un point de vue n'a pas été mentionné jusqu'ici : celui où intervient le polynôme minimal d'un élément primitif de K. On considère $F \in \mathbb{Z}[X]$ un polynôme irréductible et unitaire. On s'intéresse toujours à la factorisation d'un premier p de $\mathbb{Z}$ dans l'anneau des entiers de $K = \mathbb{Q}[X]/\langle F \rangle$. Puisque F est irréductible, son discriminant est non nul. Par conséquent, F reste sans facteur carré dans $\mathbb{Z}_p[X]$. En revanche, il n'a aucune raison d'être irréductible dans cet anneau. Introduisons la factorisation en irréductibles (distincts) de F dans $\mathbb{Z}_p[X]$:

$$F = F_1 \cdots F_r.$$

Nous allons montrer que :

Théorème 3 *Soit $F \in \mathbb{Z}[X]$ unitaire irréductible. A tout facteur irréductible $G \in \mathbb{Z}_p[X]$ de F dans $\mathbb{Z}_p[X]$ est associé un idéal premier $\mathfrak{p}$ de $\mathbb{Q}[X]/\langle F \rangle$ au dessus de p tel que $\deg G = e_{\mathfrak{p}} f_{\mathfrak{p}}$.*

Réciproquement, à tout idéal premier de $\mathbb{Q}[X]/\langle F \rangle$ au dessus de p est associé un diviseur irréductible G de F dans $\mathbb{Z}_p[X]$ et $\mathbb{Q}_p[X]/\langle G \rangle$ est le complété de $\mathbb{Q}[X]/\langle F \rangle$ pour la valeur absolue associée à $v_{\mathfrak{p}}/e_{\mathfrak{p}}$.

Preuve — L'idéal $\mathbb{Q}[X] \cap G\mathbb{Q}_p[X]$ est un idéal premier de $\mathbb{Q}[X]$ contenant $F\mathbb{Q}[X]$ donc $F\mathbb{Q}[X] = \mathbb{Q}[X] \cap G\mathbb{Q}_p[X]$. Notons $x = \overline{X}$, la classe de X modulo F, i.e. $\mathbb{Q}(x) = \mathbb{Q}[X]/\langle F \rangle$; nous venons de montrer que $\mathbb{Q}(x)$ s'injecte dans $\mathbb{Q}_p(x)$. De plus, $\mathbb{Q}_p(x)$ est aussi une extension de $\mathbb{Q}_p$ (de degré $\deg G$). La proposition 14 permet immédiatement de conclure si toutefois on s'est persuadé du fait que $\mathbb{Q}(x)$ est dense dans $\mathbb{Q}_p(x)$. Il suffit d'utiliser le fait que $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$. En effet, si $z \in \mathbb{Q}_p(x)$ est de la forme $z = \sum a_i x^i$, alors un élément $y \in \mathbb{Q}(x)$ de la forme $y = \sum b_i x^i$ où chaque $b_i \in \mathbb{Q}$ est proche de a_i est en définitive proche de z.

Réciproquement, comme on l'a vu dans la proposition 14, à tout idéal premier $\mathfrak{p}$ de $\mathbb{Q}[X]/\langle F \rangle = \mathbb{Q}(x)$ au dessus de p correspond une extension E de $\mathbb{Q}_p$ qui contient $\mathbb{Q}(x)$: c'est $\mathbb{Q}_p(x)$. En effet, comme on l'a déjà remarqué, $\mathbb{Q}(x)$ est dense dans $\mathbb{Q}_p(x)$. Soit G le polynôme minimal de x sur $\mathbb{Q}_p$; G est en fait à coefficients dans $\mathbb{Z}_p$ (car x est entier sur $\mathbb{Z}$ donc a fortiori sur $\mathbb{Z}_p$) et divise F dans $\mathbb{Q}_p[X]$ mais aussi dans $\mathbb{Z}_p[X]$. $\square$

II Une interprétation p-adique du critère de Van der Waerden-Dedekind

Les prémices de la théorie de "localisation" et "globalisation" étant (re)-posés, nous allons maintenant utiliser cette théorie pour démontrer "p-adiquement" le critère de Van der Waerden-Dedekind sous une forme assez générale. Dans le théorème 2 de [3], Chap 5, §2, n°2, la théorie générale de réduction "à la Artin" est étudiée, dans un cadre très général. En particulier, "à côté de l'inertie", traduit dans le cadre des corps de nombres, ou plutôt des polynômes à coefficients rationnels, ce théorème donne une version faible du critère de Van der Waerden-Dedekind ; cette dernière est très souvent citée et s'énonce comme suit :

Théorème 4 *Soit $F \in \mathbb{Z}[X]$ un polynôme unitaire irréductible de degré n et p un premier de $\mathbb{Z}$ qui ne divise pas le discriminant de F. Alors il existe $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, dont le type (suite croissante des longueurs des cycles) est égale à la suite des degrés (rangés par ordre croissant) des facteurs de F modulo p.*

La preuve de ce théorème est assez élémentaire[6]. Voici un énoncé du résultat (plus général, et un peu plus rare dans la littérature[7]) que nous allons démontrer :

Théorème 5 (Critère de Van der Waerden-Dedekind) *Soit K un corps de nombres et $L/\mathbb{Q}$ un corps de nombres **galoisien** de groupe de Galois Γ, contenant K. Etant donné $\mathfrak{P}$ un premier de L au dessus d'un premier p de $\mathbb{Z}$, on considère $D(\mathfrak{P})$ et $I(\mathfrak{P})$ les deux sous-groupes de Γ que sont respectivement le groupe de décomposition et le groupe d'inertie de $\mathfrak{P}$. On suppose que la décomposition de p dans K est de la forme :*

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \qquad \textit{avec} \quad N_{K/\mathbb{Q}}(\mathfrak{p}_i) = p^{f_i}.$$

On considère l'action de Γ sur $\underline{K} = \mathrm{Hom}_{\mathbb{Q}}(K, L)$, par composition à gauche, alors $\underline{K}$ se décompose en g $D(\mathfrak{P})$-orbites de longueur respective $e_i f_i$, et chacune d'entre elles se décompose en f_i $I(\mathfrak{P})$-orbites de longueur e_i.

[6] Le lecteur peut par exemple consulter [14], Chap 6, §2, Exemple 7.

[7] T.Kondo l'énonce et l'utilise dans [12], mais ne le redémontre pas. Pour la preuve, il renvoie le lecteur à un ouvrage écrit en japonais ou à Van der Waerden lui même...

La preuve permet de réinvestir les connaissances des sections précédentes. En fait, nous ne ferons que très rarement appel à des propriétés bien précises. En revanche, le contexte étant le même, “les bulles”, du début de ce papier, seront perpétuellement sous-jacentes.

Enfin, l'exposé qui suit est ponctué de rappels de résultats généraux avec ou sans preuves. Cependant la compréhension des démonstrations non présentées ne posent aucun problème pour quelqu'un dominant les prémices cités ci-avant. Autant que faire se peut, je donnerai des références précises, où trouver toutes les démonstrations. Les paragraphes concernant ces rappels commencent par la mention “*Intermède général*” et se terminent par “*Fin de l'intermède*”.

Pour commencer, une fois n'est pas coutume, nous allons étudier un exemple.

II.1 Etude d'un exemple

Le critère de Van der Waerden-Dedekind sous sa forme la plus faible est très souvent utilisé pour cerner le groupe de Galois d'un polynôme $F \in \mathbb{Z}[X]$. On factorise ce dernier modulo un certain de nombre de premiers **ne divisant pas le discriminant de** F de façon à éliminer certains sous-groupes. Grâce au théorème de densité de Cebotarev, on sait que l'on peut déterminer le type des permutations constituant le groupe de Galois au bout d'un certain nombre de tirages (ce qui ne résoud pas le problème de la détermination du groupe de Galois, puisqu'il existe des sous-groupes non conjugués de S_n constitués de permutations de même type). Prenant le contre-pied de la méthode précédente, nous allons examiner, ici, la factorisation des premiers **ramifiés** dans le corps de nombres engendré par une racine du polynôme F. Il se profile déjà une difficulté supplémentaire : quand p ne divise pas le discriminant de F alors la factorisation du polynôme F modulo p reflète celle de de p dans le corps de nombres associé à F ; ce n'est pas toujours le cas quand p se ramifie, ni même quand $p \mid \mathrm{dis}(F) \ldots$

• Soit $F(X) = X^5 + 20X + 16$; F est irréductible sur $\mathbb{Z}$ et $\mathrm{dis}(F) = 2^{16}5^6$ est un carré, par suite $\mathrm{Gal}(F/\mathbb{Q})$ est un sous-groupe transitif de A_5. Ces derniers sont au nombre de trois :

$$(C_5, \#5) \subset (D_5, \#10) \subset (A_5, \#60)$$

Dans le corps de nombres, K, engendré par une racine de F, le premier 2 se factorise sous la forme (résultat obtenu grâce au système de Calcul Formel MAGMA) :

$$\langle 2 \rangle = \mathfrak{p}^4\mathfrak{q}, \qquad \text{avec} \qquad f_{\mathfrak{p}} = f_{\mathfrak{q}} = 1$$

Par conséquent, d'après le critère de Van der Waerden-Dedekind, si $\mathfrak{P}$ est un premier de K^{gal} (i.e. le corps de décomposition de F), $I(\mathfrak{P})$ est un sous-groupe transitif de S_4 donc de A_4 puisque $I(\mathfrak{P})$ est aussi un sous-groupe de $\mathrm{Gal}(F/\mathbb{Q})$ qui est constitué de permutations paires (en tant que permutations de $\underline{K}$). Ainsi,

$$\#I(\mathfrak{P}) \mid 12 \qquad \text{donc} \qquad \#I(\mathfrak{P}) \in \{2, 3, 4, 6, 12\}$$

Mais comme A_4 ne contient aucun sous-groupe transitif de cardinal 2, nécessairement, $\#I(\mathfrak{P})$ est soit divisible par 3 soit divisible par 4 ; il en est donc de même de $\#\,\mathrm{Gal}(F/\mathbb{Q})$, qui par conséquent ne peut être que A_5.

II.2 Une preuve p-adique du critère de Van der Waerden-Dedekind

Soit L une extension galoisienne d'un corps K de groupe de Galois Γ. On considère E une K-extension de degré n contenue dans L :

$$\begin{tikzcd} L \arrow[dd, dash, "\Gamma"'] \arrow[dr, dash] & \\ & E \arrow[dl, dash, "n"] \\ K & \end{tikzcd} \qquad\qquad \underline{E} = \mathrm{Hom}_K(E, L)$$

Alors le groupe Γ opère **transitivement** sur $\underline{E}$ par composition à gauche :

$$\begin{array}{ccc} \Gamma \times \underline{E} & \longrightarrow & \underline{E} \\ (\lambda, \sigma) & \longmapsto & \lambda \circ \sigma \end{array}$$

De plus, cette opération est fidèle si et seulement si L est la clôture galoisienne de E.

Remarques

1. Plutôt que d'imposer E inclus dans L, il est préférable de supposer que le corps E **s'injecte** dans le corps L ; le corps L est alors une E-extension au sens de la définiton générale d'extension de corps. Si, comme ce sera souvent le cas dans la suite, E est inclus dans L, alors E s'injecte bien évidemment dans L et on a une injection distinguée, à savoir celle que l'on qualifie communément de **canonique**.

2. En réalisant, l'extension E par un élément primitif, i.e. en écrivant $E = K(x)$, on retrouve l'action usuelle du groupe Γ sur les racines d'un polynôme, à savoir le polynôme minimal de x sur K.

Nous allons maintenant utiliser la réalisation précédente d'un groupe de Galois pour établir le critère de Van der Waerden-Dedekind. Pour cela, on considère K un corps de nombres et L une extension **galoisienne** de $\mathbb{Q}$ contenant K. On note :

$$\Gamma = \mathrm{Gal}(L/\mathbb{Q}) \qquad \text{et} \qquad \underline{K} = \mathrm{Hom}_{\mathbb{Q}}(K, L).$$

Fixons $\mathfrak{P}$, un idéal premier de L au dessus d'un premier p de $\mathbb{Z}$; cela revient à se fixer une valeur absolue sur L, à savoir $|\ |_{\mathfrak{P}}$ prolongeant la valeur absolue p-adique. Considérons $D(\mathfrak{P})$ le groupe de décomposition de $\mathfrak{P}$; $D(\mathfrak{P})$ n'est rien d'autre que le sous-groupe de Γ qui préserve la valeur absolue $|\ |_{\mathfrak{P}}$. En effet,

Proposition 16 *Soit K et K' deux corps de nombres et σ un élément de $\mathrm{Hom}_{\mathbb{Q}}(K, K')$. On considère $\mathfrak{p}$ et $\mathfrak{p}'$ deux idéaux premiers de K et K' respectivement ; on note $|\ |$ la valeur absolue sur K associée à $\mathfrak{p}$ et $|\ |'$ celle sur K' associée à $\mathfrak{p}'$. Alors σ préserve les valeurs absolues, i.e. $|\sigma(x)|' = |x|$, si et seulement si $\sigma^{-1}(\mathfrak{p}') = \mathfrak{p}$.*

Preuve — On sait que $\sigma^{-1}(\mathfrak{p}')$ est un idéal premier de K. Il suffit donc de vérifier (par exemple) que $\sigma^{-1}(\mathfrak{p}') \subset \mathfrak{p}$. Mais si $x \in K$ vérifie $\sigma(x) \in \mathfrak{p}'$ alors $|\sigma(x)|' < 1$ et donc $|x| < 1$. L'élément x étant nécessairement entier (car $\sigma^{-1}(\mathcal{O}') = \mathcal{O}$ où $\mathcal{O}$ et $\mathcal{O}'$ sont les anneaux d'entiers respectifs de K et K'), on a bien $x \in \mathfrak{p}$. $\square$

En particulier, si on considère L un corps de nombres galoisien, et si on applique la proposition précédente à $K = K' = L$, on obtient ce que l'on voulait, c'est-à-dire :

Corollaire 1 *Soit L un corps de nombres galoisien. Pour tout premier $\mathfrak{P}$ de L, le sous-groupe de $\mathrm{Gal}(L/\mathbb{Q})$ qui préserve la valeur absolue $|\ |_{\mathfrak{P}}$ associée à $\mathfrak{P}$ n'est rien d'autre que le groupe de décomposition de $\mathfrak{P}$, noté $D(\mathfrak{P})$.*

Les orbites de $\underline{K}$ sous l'action de $D(\mathfrak{P})$

Cela étant, nous allons maintenant déterminer les orbites de $\underline{K}$ sous l'action de $D(\mathfrak{P})$. Remarquons que tout élément $\sigma \in \underline{K}$ induit sur K un idéal premier au dessus de p, via $\sigma^{-1}(\mathfrak{P})$, ou encore, de manière équivalente, une valeur absolue sur K (prolongeant la valeur absolue p-adique) via $|\ |_{\mathfrak{P}} \circ \sigma$. On obtient ainsi une partition de $\underline{K}$ par :

$$\underline{K} = \bigvee_{\mathfrak{p} \in \mathrm{Spec}_p(K)} \{\sigma \in \underline{K},\ \sigma^{-1}(\mathfrak{P}) = \mathfrak{p}\} = \bigvee_{\mathfrak{p} \in \mathrm{Spec}_p(K)} \{\sigma \in \underline{K},\ |\ |_{\mathfrak{P}} \circ \sigma = |\ |_{\mathfrak{p}}\}$$

où, je le rappelle, $\mathrm{Spec}_p(K)$ désigne l'ensemble des premiers de K au dessus de p.

Vérifions, que cette partition correspond, en fait, aux orbites de $\underline{K}$ sous l'action de $D(\mathfrak{P})$. Soit $\mathfrak{p}$ un premier de K au dessus de p. Tout élément $\sigma \in \underline{K}$ tel que $\sigma^{-1}(\mathfrak{P}) = \mathfrak{p}$ se prolonge en un élément $\widehat{\sigma} \in \mathrm{Hom}_{\mathbb{Q}_p}(K_{\mathfrak{p}}, L_{\mathfrak{P}})$ comme le montre le résultat suivant :

Intermède général

Proposition 17 *Soit L un corps muni d'une valeur absolue $|\ |_L$, et L/K une extension galoisienne. On considère E une K-extension munie d'une valeur absolue $|\ |_E$. L'application de restriction,*

$$\varphi : \begin{array}{ccc} \mathrm{Hom}_{\widehat{K}}(\widehat{E}, \widehat{L}) & \longrightarrow & \mathrm{Hom}_K(E, L) \\ \sigma & \longmapsto & \sigma_{|E} \end{array}$$

est bien définie. De plus, φ est injective et $\mathrm{Hom}_{\widehat{K}}(\widehat{E}, \widehat{L})$ s'identifie, par φ, au sous-groupe de $\mathrm{Hom}_K(E, L)$ qui préserve les valeurs absolues.

Preuve — Tout d'abord, s'il n'existe pas d'homomorphisme $\tau \in \mathrm{Hom}_K(E, L)$ qui préserve les valeurs absolues, i.e. $|\tau(x)|_L = |x|_E$, alors les ensembles d'homomorphimes cités sont tous vides, ce qui rend la proposition immédiate (et inintéressante). On se place donc dans le cas contraire et on considère $\tau \in \mathrm{Hom}_K(E, L)$ un K-homomorphisme qui préserve les valeurs absolues. En particulier, τ est uniformément continu sur E. Le corps E est dense dans $\widehat{E}$, $\widehat{L}$ est complet ; ainsi, τ se prolonge en un K-homomorphisme, $\widehat{\tau} \in \mathrm{Hom}_K(\widehat{E}, \widehat{L})$ (c.f. [8], Chap III §15). Nécessairement $\widehat{\tau} \in \mathrm{Hom}_{\widehat{K}}(\widehat{E}, \widehat{L})$. Le corps $\widehat{E}$ s'injecte bien dans $\widehat{L}$.

Cela étant, montrons que l'application φ est définie. L'extension L/K étant galoisienne et E s'injectant dans L (τ est une telle injection), $\mathrm{Hom}_K(E, \widehat{L}) = \mathrm{Hom}_K(E, L)$. Ainsi, pour tout $\sigma \in \mathrm{Hom}_{\widehat{K}}(\widehat{E}, \widehat{L})$, $\sigma_{|E} \in \mathrm{Hom}_K(E, L)$. L'application φ est bien définie. Elle est de plus injective par densité. Il reste à caractériser l'image de φ. Pour cela, on remarque que tout $\sigma \in \mathrm{Hom}_{\widehat{K}}(\widehat{E}, \widehat{L})$ conserve la valeur absolue (à cause de l'unicité du prolongement de $|\ |$ à $\widehat{L}$) ; il en est donc de même pour $\sigma_{|E}$. Réciproquement, si $\sigma \in \mathrm{Hom}_K(E, L)$ préserve la valeur absolue, alors on peut le prolonger en un homomorphisme de $\mathrm{Hom}_{\widehat{K}}(\widehat{E}, \widehat{L})$ comme nous l'avons déjà fait pour τ au début de cette preuve. $\square$

En particulier, si $E = L$, alors l'injection canonique vérifie bien évidemment l'hypothèse de la proposition précédente. On obtient alors le résultat suivant :

Corollaire 2 *Soit L/K une extension galoisienne de corps muni d'une valeur absolue $|\ |$. Alors l'extension $\widehat{L}/\widehat{K}$ est galoisienne ; $\mathrm{Gal}(\widehat{L}/\widehat{K})$ s'identifie canoniquement (par restriction) au sous-groupe de $\mathrm{Gal}(L/K)$ qui préserve la valeur absolue.*

Fin de l'intermède

Des deux résultats précédents, nous pouvons tirer plusieurs renseignements relatifs à notre situation. Tout d'abord, étant donné $\mathfrak{p}$ un premier de K, tout $\sigma \in \underline{K}$ tel que $\sigma^{-1}(\mathfrak{P}) = \mathfrak{p}$ se prolonge en un élément $\widehat{\sigma} \in \mathrm{Hom}_{\mathbb{Q}_p}(K_\mathfrak{p}, L_\mathfrak{P})$. De plus, on a un isomorphisme canonique (la restriction) entre :

$$\mathrm{Hom}_{\mathbb{Q}_p}(K_\mathfrak{p}, L_\mathfrak{P}) \simeq \{\sigma \in \underline{K},\ \sigma^{-1}(\mathfrak{P}) = \mathfrak{p}\} \tag{2}$$

De plus, en vertu des corollaires 1 et 2, l'extension $L_\mathfrak{P}/\mathbb{Q}_p$ est galoisienne de groupe de Galois canoniquement isomorphe à $D(\mathfrak{P})$. Par suite, $D(\mathfrak{P})$ ($= \mathrm{Gal}(L_\mathfrak{P}/\mathbb{Q}_p)$) opère transitivement sur $\underline{K_\mathfrak{p}} = \mathrm{Hom}_{\mathbb{Q}_p}(K_\mathfrak{p}, L_\mathfrak{P})$.

Dès lors, étant donnés $\sigma, \tau \in \underline{K}$ tels que $\sigma^{-1}(\mathfrak{P}) = \mathfrak{p}$ et $\tau^{-1}(\mathfrak{P}) = \mathfrak{p}$, alors il existe $\widehat{\lambda} \in D(\mathfrak{P})$ tel que $\widehat{\lambda} \circ \widehat{\tau} = \widehat{\sigma}$; restreint à K, on obtient ce que l'on voulait, c'est-à-dire σ et τ $D(\mathfrak{P})$-conjugués.

En résumé, à chaque orbite de $\underline{K}$ sous $D(\mathfrak{P})$, correspond un idéal premier de K ou de manière équivalente une valeur absolue sur K. Plus précisément,

- si $\mathfrak{p}$ est un premier de K (au dessus de p), alors l'orbite de $\underline{K}$ sous $D(\mathfrak{P})$ associée à $\mathfrak{p}$ est constituée des $\mathbb{Q}$-morphismes $\sigma \in \underline{K}$ tels que $\sigma^{-1}(\mathfrak{P}) = \mathfrak{p}$
- de manière équivalente, si $|\ |$ est une valeur absolue sur K (prolongeant la valeur absolue p-adique), alors l'orbite de $\underline{K}$ sous $D(\mathfrak{P})$ associée à $|\ |$ est constituée des $\mathbb{Q}$-morphismes $\sigma \in \underline{K}$ tels que $|\ |_\mathfrak{P} \circ \sigma = |\ |$.

Enfin compte tenu de l'isomorphisme 2, l'orbite de $\underline{K}$ sous $D(\mathfrak{P})$, associée à un idéal premier $\mathfrak{p}$ de K, a autant d'éléments que $\mathrm{Hom}_{\mathbb{Q}_p}(K_\mathfrak{p}, L_\mathfrak{P})$, c'est-à-dire, l'extension $L_\mathfrak{P}/\mathbb{Q}_p$ étant galoisienne, $[K_\mathfrak{p} : \mathbb{Q}_p]$, ou encore, avec les notations usuelles $e_\mathfrak{p} f_\mathfrak{p}$. En conclusion, nous venons d'établir que :

Proposition 18 *Conservant les hypothèses du début, si p, dans K, se factorise de la manière suivante :*

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \qquad \textit{avec} \quad N(\mathfrak{p}_i) = p^{f_i} \ ;$$

alors $\underline{K}$ se décompose en g $D(\mathfrak{P})$-orbites, de longueurs respectives $e_i f_i$.

Les orbites de $\underline{K}$ sous l'action de $I(\mathfrak{P})$

Etudions, désormais, de plus près chacune des orbites de $\underline{K}$ sous l'action de $D(\mathfrak{P})$. En particulier on s'intéresse à l'action du **groupe d'inertie**, noté $I(\mathfrak{P})$, sur chacune d'entre elles. Pour fixer les idées, polarisons notre étude sur l'orbite de l'injection canonique $i : K \hookrightarrow L$, c'est-à-dire l'orbite associée à l'idéal premier $\mathfrak{p} = \mathfrak{P} \cap K$ ou encore à la valeur absolue $|\ |_\mathfrak{P}$ restreinte à K. On sait que les éléments de cette orbite sont en bijection avec les éléments de $\mathrm{Hom}_{\mathbb{Q}_p}(K_{\mathfrak{p}}, L_{\mathfrak{P}})$. Ainsi, "en complétant", on ramène le problème à l'étude de la situation suivante (on "enlève les indices") : on dispose d'une extension galoisienne de $\mathbb{Q}_p$, $L_{\mathfrak{P}}$ que l'on note encore L, de groupe de Galois Γ (c'est $D(\mathfrak{P})$) et d'une extension intermédiaire E (c'est $K_{\mathfrak{p}}$) :

$$\begin{tikzcd} L \arrow[dd, dash, "\Gamma"'] \arrow[dr, dash] & \\ & E \arrow[dl, dash] \\ \mathbb{Q}_p & \end{tikzcd} \qquad \text{(Situation locale)}$$

On cherche les orbites du groupe d'inertie, $I = I(L/\mathbb{Q}_p)$ (c'est $I(\mathfrak{P})$), sur $\underline{E} = \mathrm{Hom}_{\mathbb{Q}_p}(E, L)$.

Commençons par caractériser le groupe d'inertie.

Intermède général

Tout d'abord, rappelons un lemme élémentaire de théorie des groupes :

Lemme 4 *Soit G un groupe opérant* ***transitivement*** *sur un ensemble A et H un sous-groupe* ***distingué*** *de G. Alors G permute transitivement les H-orbites de A. En particulier, si A est fini, toutes les H-orbites ont le même cardinal, e, et si f est le nombre de H-orbites, on a $\#A = ef$.*

Preuve — Tout repose sur la remarque suivante (qui découle du fait que H est distingué dans G) : $Hga = gHa$ pour tout $g \in G$ et $a \in A$. $\square$

Dans un deuxième temps, il nous faut rappeler des résultats relatifs à la théorie des corps locaux qui figurent pour la plupart dans [21], Chap III, §5. Durant le reste de cet intermède, K désigne un corps complet pour une valuation discrète, i.e. un corps local, dont le corps résiduel, k, est supposé parfait.

Tout d'abord, si L est une extension **non ramifiée** de K, i.e. $e(L/K) = 1$, alors $\mathrm{Aut}_K(L) \simeq \mathrm{Aut}_k(l)$ où k et l sont les corps résiduels respectifs de K et L. Ce résultat est un corollaire du théorème 3 de la section de [21] citée ci-avant[8]. En particulier, si l'extension l/k est galoisienne, il en est de même de l'extension L/K. Par conséquent, si les corps résiduels sont finis (ce qui est le cas dans notre exemple), alors toutes les extensions non ramifiées de K sont galoisiennes (et même cycliques).

Ensuite, étant donnée L/K une extension finie, il existe une K-extension L_0 non ramifiée maximale contenue dans L (c.f. Corollaire 3, id.). De plus, L/L_0 est **totalement ramifiée**, i.e. $f(L/L_0) = 1$ et, avec des notations implicites on a :

$$\overbrace{K \qquad\quad L_0}^{f(L/K)}\overbrace{\qquad\quad L}^{e(L/K)}$$

Enfin, pour une extension galoisienne de K, on peut interpréter le groupe d'inertie de la manière suivante :

Proposition 19 *Soit L une extension galoisienne de K de groupe de galois Γ. On considère L_0 la K-extension* ***non ramifiée*** *maximale contenue dans L. Alors le groupe d'inertie $I(L/K)$ est égal au groupe de Galois $\mathrm{Gal}(L/L_0)$; de plus, l'extension L_0/K est galoisienne et le morphisme de restriction $\Gamma \longrightarrow \mathrm{Gal}(L_0/K)$ induit un isomorphisme de :*

$$\Gamma/I(L/K) \simeq \mathrm{Gal}(L_0/K)$$

Fin de l'intermède

Revenons aux orbites de $\underline{E}$ sous l'action de I. Appelons L_0 la plus grande $\mathbb{Q}_p$-extension **non ramifiée** contenue dans L et E_0 celle contenue dans E. Nécessairement $E_0 \subset L_0$ et cette extension est non ramifiée. Un petit schéma pour fixer les idées :

$$\begin{tikzcd} L \arrow[d, dash, "\mathrm{tr}"'] \arrow[dr, dash] & \\ L_0 \arrow[dd, dash, "\mathrm{nr}"'] \arrow[dr, dash, "\mathrm{nr}"'] & E \arrow[d, dash, "\mathrm{tr}"] \\ & E_0 \arrow[dl, dash, "\mathrm{nr}"] \\ \mathbb{Q}_p & \end{tikzcd} \qquad \text{avec :} \quad \begin{array}{c} \mathrm{tr} = \text{totalement ramifiée} \\ \mathrm{nr} = \text{non ramifiée} \end{array}$$

[8]La preuve de ce théorème utilise un cas particulier du lemme de Hensel, sur lequel nous reviendrons longuement dans la section III

D'après ce qui précède, l'extension $L_0/\mathbb{Q}_p$ est galoisienne (même cyclique) et $I = \mathrm{Gal}(L/L_0)$; par suite, I est un sous-groupe distingué de Γ. Ce dernier opère donc transitivement sur les I-orbites de $\underline{E}$. Elles ont donc toutes le même cardinal ; déterminons ce dernier. Nous pouvons polariser notre attention sur l'orbite de l'injection canonique. On remarque que tout élément de cette orbite appartient à $\mathrm{Hom}_{E_0}(E, L)$ car $E_0 \subset L_0$; en fait, $I.i = \mathrm{Hom}_{E_0}(E, L)$. Pour tout $\sigma \in \mathrm{Hom}_{E_0}(E, L)$, il faut donc vérifier que l'on peut prolonger σ en un L_0-homomorphisme. En fait, E et L_0 sont deux sous-extensions de l'extension L/E_0. Nous disposons donc de deux E_0-homomorphismes, à savoir $\sigma \in \mathrm{Hom}_{E_0}(E, L)$ et $i \in \mathrm{Hom}_{E_0}(L_0, L)$, l'injection canonique de L_0 dans L, et nous voulons $\lambda \in \Gamma$ qui prolonge les deux. Cette situation peut être étudiée dans un cadre plus général.

Intermède général

Le problème est le suivant : étant donnés K/k une extension de corps, E/k et F/k deux extensions intermédiaires, $\sigma \in \mathrm{Hom}_k(E, K)$ et $\tau \in \mathrm{Hom}_k(F, K)$:

$$\begin{tikzcd}
 & E \arrow[dr, "\sigma"] & \\
k \arrow[ur, dash] \arrow[r, dash] \arrow[dr, dash] & k(E,F) \arrow[r, dotted, "?"] & K \\
 & F \arrow[ur, "\tau"'] &
\end{tikzcd}$$

dans quelle mesure est-il possible de trouver $\lambda \in \mathrm{Hom}_k(k(E, F), K)$ qui prolonge à la fois σ et τ sur E et F respectivement ? Ce genre de problème est résoluble, par exemple, dans le cas suivant :

Lemme 5 *Sous les hypothèses précédentes, si on suppose de plus que E et F sont* ***linéairement disjointes*** *sur k, alors il existe un prolongement à la k-algèbre $k[E, F]$ qui coincide avec σ et τ sur E et F respectivement.*

Ensuite, dans notre cadre, il sera possible de conclure en remarquant que E et F étant de plus supposées **algébriques** sur k, alors $k[E, F] = EF = k(E, F)$.

Le côté algébrique des extensions est évidemment vérifié. Cependant, il n'a, pour l'instant, jamais été question d'extensions linéairement disjointes ; pourtant :

Proposition 20 *Soient T/k et N/k deux extensions finies d'un* ***corps local*** *k telles que T/k soit totalement ramifiée et N/k soit non ramifiée. Alors T et N sont linéairement disjointes sur k.*

Preuve — Notons $K = k(T, N)$; il suffit de montrer que $[K : k] \geqslant [T : k][N : k]$. Avec des notations implicites, nécessairement, $e(K/k) \geqslant e(T/k) = [T : k]$ et $f(K/k) \geqslant f(N/k) = [N : k]$. Ainsi,

$$[K : k] = e(K/k)f(K/k) \geqslant [T : k][N : k],$$

d'où le résultat. □

Fin de l'intermède

Revenons maintenant à la situation précédente. Je rappelle que l'on dispose de deux sur-corps de E_0, L_0 et E (tous deux inclus dans L) tels que :

$$\overbrace{E_0 \qquad\qquad\qquad E}^{\text{tot. ramifiée}} \subset L \qquad \text{et} \qquad \overbrace{E_0 \qquad\qquad\qquad L_0}^{\text{non ramifiée}} \subset L$$

De plus, on s'est fixé $\sigma \in \underline{E}$, et on considère i, l'injection canonique de L_0 dans L :

$$\sigma : E \longrightarrow L \qquad \text{et} \qquad i : L_0 \hookrightarrow L$$

D'après ce qui précède, E et L_0 sont linéairement disjointes sur E_0, ainsi, il existe $\lambda \in \mathrm{Hom}_{E_0}(E_0(E, L_0), L)$ tel que $\lambda_{|E} = \sigma$ et $\lambda_{|L_0} = i$. Par suite, n'importe quel prolongement de λ à L nous donne bien un élément de $I = \mathrm{Gal}(L/L_0)$ tel que $\lambda_{|E} = \sigma$, ce que l'on voulait.

En conclusion, nous venons d'établir la version générale du critère de Van der Waerden-Dedekind énoncée ci-avant.

II.3 Lien avec l'énoncé du premier critère

L'objet de cette section, est de retrouver la forme "faible" du critère de Van der Waerden-Dedekind (i.e. le théorème 4) à partir du résultat que nous venons d'établir. Je considère donc $F \in \mathbb{Z}[X]$ un polynôme unitaire irréductible de degré n et p un premier de $\mathbb{Z}$ qui ne divise pas le discriminant de F. Soit θ une racine de F et $\theta_1 = \theta, \dots, \theta_n$ ses conjugués. Avec les notations du théorème précédent, on pose :

$$K = \mathbb{Q}(\theta) \qquad \text{et} \qquad L = \mathbb{Q}(\theta_1, \dots, \theta_n).$$

L'extension $L/\mathbb{Q}$ est bien sûr galoisienne de groupe de Galois égal à $\mathrm{Gal}(F/\mathbb{Q})$. Comme p ne divise pas le discriminant de F, la factorisation de F modulo p, $F \equiv F_1 \dots F_g \mod p$, reflète donc (théorème de Kummer) celle de p dans K. Ainsi, dans K,

$$\langle p \rangle = \mathfrak{p}_1 \cdots \mathfrak{p}_g \qquad \text{avec :} \quad N(\mathfrak{p}_\mathfrak{i}) = p^{\deg F_i}.$$

Par conséquent, étant donné $\mathfrak{P}$ un premier de L (au dessus de p), d'après le théorème 5, $\underline{K}$ se décompose en g $D(\mathfrak{P})$-orbites de longueurs respectives $\deg F_i$. Pour finir, p étant supposé **non ramifié** (car p ne divise pas le discriminant de F), $D(\mathfrak{P})$ est **cyclique**, engendré par $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ (c.f. [14], Chap VII §2, Proposition 2.8). Par suite, les $D(\mathfrak{P})$-orbites de $\underline{K}$ sont exactement les longueurs des cycles de σ. Le groupe de Galois $\mathrm{Gal}(F/\mathbb{Q})$ contient donc une permutation dont le type correspond à la suite des degrés des facteurs de F modulo p.

Remarque – Plutôt que de supposer que le premier p de $\mathbb{Z}$ ne divise pas le discriminant de F, il suffit de supposer que p ne divise pas le discriminant de l'extension $K/\mathbb{Q}$, ou, ce qui revient au même, discriminant de l'extension $L/\mathbb{Q}$ (i.e. p est non ramifié). Cela donne une nouvelle version "intermédiaire" du critère de Van der Waerden-Dedekind assez souvent citée.

II.4 Premiers de faible exposant dans le discriminant d'un corps de nombres

II.4.1 Passage du local au global

Dans la preuve du critère de Van der Waerden-Dedekind, nous sommes partis d'une situation globale et nous avons "localisé". Inversement, dans cette section, nous allons faire en sorte de "globaliser" des informations locales. Plus précisément, on considère la situation désormais classique, à savoir L un corps de nombres galoisien de groupe de Galois Γ et $K/\mathbb{Q}$ une extension intermédiaire de degré n :

$$\begin{tikzcd} L \arrow[dd, dash, "\Gamma"'] \arrow[dr, dash] & \\ & K \arrow[dl, dash, "n"] \\ \mathbb{Q} & \end{tikzcd} \qquad\qquad \underline{K} = \mathrm{Hom}_{\mathbb{Q}}(K, L)$$

Un premier p de $\mathbb{Z}$ est fixé une fois pour toutes, ainsi qu'un premier $\mathfrak{P}$ de L au dessus de p. Introduisons maintenant la factorisation de p dans le corps K :

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \qquad \text{avec} \quad N_{K/\mathbb{Q}}(\mathfrak{p}_i) = p^{f_i}$$

On pose, pour alléger, $K_i = K_{\mathfrak{p}_\mathfrak{i}}$. Pour chaque i, on dispose de $n_i = e_i f_i$ $\mathbb{Q}_p$-homomorphismes $K_i \to L_\mathfrak{P}$; on note $\underline{K_i}$ cet ensemble. Chaque $\underline{K_i}$ est canoniquement isomorphe (par restriction) au sous-ensemble des $\mathbb{Q}$-homomorphismes σ de $\underline{K}$ tels que $\sigma^{-1}(\mathfrak{P}) = \mathfrak{p}_i$. De plus, les $\underline{K_i}$ forment une partition de $\underline{K}$; ce sont aussi les $D(\mathfrak{P})$-orbites de $\underline{K}$. On a donc le diagramme commutatif suivant :

$$\begin{tikzcd} D(\mathfrak{P}) \arrow[r] \arrow[d, hook, "\substack{\text{injection} \\ \text{canonique}}"'] & \prod_{i=1}^{g} \mathrm{Perm}(\underline{K_i}) \arrow[d, hook, "\substack{\text{injection} \\ \text{canonique}}"] \\ \Gamma \arrow[r] & \mathrm{Perm}(\underline{K}) \end{tikzcd}$$

Dès que la flèche horizontale du bas est injective, l'autre flèche horizontale l'est aussi. En particulier, si L est la clôture galoisienne de K, les deux flèches horizontales sont injectives.

Mieux, si on introduit K_i^{gal} le compositum des $\sigma(K_i)$ pour $\sigma \in \underline{K_i}$ alors K_i^{gal} est inclus dans $L_{\mathfrak{P}}$; c'est aussi la clôture galoisienne de n'importe quel $\sigma(K_i)$ pour $\sigma \in \underline{K_i}$. On a alors deux nouveaux diagrammes commutatifs, le deuxième s'obtenant par restriction aux groupes d'inertie :

$$\begin{array}{ccc} D(\mathfrak{P}) = \mathrm{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_p) & \longrightarrow & \prod_{i=1}^{g} \mathrm{Gal}(K_i^{\text{gal}}/\mathbb{Q}_p) \\ \downarrow & & \downarrow \\ \mathrm{Perm}(\underline{K}) & \longleftarrow & \prod_{i=1}^{g} \mathrm{Perm}(\underline{K_i}) \end{array} \qquad \begin{array}{ccc} I(\mathfrak{P}) = I(L_{\mathfrak{P}}/\mathbb{Q}_p) & \longrightarrow & \prod_{i=1}^{g} I(K_i^{\text{gal}}/\mathbb{Q}_p) \\ \downarrow & & \downarrow \\ \mathrm{Perm}(\underline{K}) & \longleftarrow & \prod_{i=1}^{g} \mathrm{Perm}(\underline{K_i}) \end{array} \qquad (3)$$

Les deux flèches du haut ne sont rien d'autre que "le produit des restrictions". Les flèches verticales ne font que traduire la réalisation, précisée au début de cette section d'un groupe de Galois sur un ensemble d'homomorphismes. Quant aux deux flèches horizontales du bas, elles ne font appel qu'à de la petite théorie des ensembles. Enfin, si $L = K^{\text{gal}}$, alors $D(\mathfrak{P})$ s'injecte dans $\mathrm{Perm}(\underline{K})$; par suite les deux flèches du haut, ainsi que les diagonales, sont injectives.

Remarque – Cela montre de plus que si $L = K^{\text{gal}}$, alors $L_{\mathfrak{P}}$ est le compositum des K_i^{gal}, pour $1 \leqslant i \leqslant g$. En effet, tout automorphisme $\sigma \in \mathrm{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_p)$ qui est trivial sur les K_i^{gal} est, en vertu du diagramme précédent, trivial ; d'où l'égalité voulue. En fait, on peut retrouver ce résultat, grâce au refrain : "le complété du compositum est égal au compositum des complétés" (c.f. section I.4.4, pour un énoncé plus précis). En effet, ici, L est le compositum des conjugués de K :

$$L = \mathbb{Q}[\sigma(K),\ \sigma \in \underline{K}] \qquad \text{donc :} \qquad L_{\mathfrak{P}} = \mathbb{Q}_p[(\sigma(K))_{\mathfrak{P}\cap\sigma(K)}\ \sigma \in \underline{K}]$$

En utilisant de nouveau la partition $\underline{K} = \bigvee_{1\leqslant i\leqslant g} \underline{K_i}$, on retrouve l'égalité : $L_{\mathfrak{P}} = K_1^{\text{gal}} \cdots K_g^{\text{gal}}$.

Ainsi, connaissant les groupes d'inertie des extensions locales $K_i^{\text{gal}}/\mathbb{Q}_p$ pour $1 \leqslant i \leqslant g$, on en déduit directement des précisions sur le groupe d'inertie global, à savoir $I(\mathfrak{P})$. C'est cette stratégie que nous allons suivre à partir de maintenant. En particulier, nous nous intéressons aux groupes d'inertie de premiers $\mathfrak{P}$ au dessus d'un premier p dont l'exposant dans la décomposition du discriminant de l'extension $K/\mathbb{Q}$ est petit (mais qui figure toutefois dans cette décomposition). C'est pourquoi, je fais intervenir à ce stade un nouvel invariant du corps de nombres K, à savoir l'exposant de p dans la décomposition de $\mathrm{dis}(K)$ (sous-entendu sur $\mathbb{Q}$) ; posons :

$$m = v_p(\operatorname{dis} K)$$

Compte tenu de la stratégie envisagée, il convient une nouvelle fois d'assurer la bascule entre le local et le global pour cet invariant. De manière concise, on peut reformuler les résultats, de la première section de ce document, en donnant le $\mathbb{Q}_p$-isomorphisme de $\mathbb{Q}_p$-algèbres entre :

$$K \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \prod_{i=1}^{g} K_i$$

Du point de vue des dimensions, on retrouve l'égalité (déjà rencontrée au début de ce papier) :

$$n = \dim_{\mathbb{Q}} K = \dim_{\mathbb{Q}_p} K \otimes_{\mathbb{Q}} \mathbb{Q}_p = \sum_{i=1}^{g} \dim_{\mathbb{Q}_p} K_i = \sum_{i=1}^{g} n_i$$

ou plus légèrement, la dimension globale est égale à la somme des dimensions locales. De plus, côté anneaux d'entiers (c.f. [21], Chap II, §3, Proposition 4), on a :

$$\mathcal{O}(K) \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \prod_{i=1}^{g} \mathcal{O}(K_i),$$

où la notation $\mathcal{O}(\bullet)$ désigne l'anneau des entiers de $\bullet$. Ainsi,

$$\operatorname{dis} K = \prod_{i=1}^{g} \operatorname{dis} K_i \qquad \text{d'où :} \qquad v_p(\operatorname{dis} K) = \sum_{i=1}^{g} v_p(\operatorname{dis} K_i)$$

Cette égalité assure le passage du local au global que nous voulions.

Il nous reste donc désormais à étudier les extensions locales dont le discriminant a une valuation p-adique petite. Ceci est l'objet de la section suivante :

II.4.2 Etude de la situation locale

On se place donc en situation locale : E est un corps de nombres p-adiques ; les notations sont regroupées dans la ligne suivante :

$$\Gamma = \mathrm{Gal}(E^{\mathrm{gal}}/\mathbb{Q}_p), \quad I = I(E^{\mathrm{gal}}/\mathbb{Q}_p), \qquad \begin{tikzcd} E^{\mathrm{gal}} \arrow[dd, dash, "\Gamma"'] \arrow[dr, dash] & \\ & E \arrow[dl, dash, "n=ef"] \\ \mathbb{Q}_p & \end{tikzcd} \qquad \underline{E} = \mathrm{Hom}_{\mathbb{Q}_p}(E, E^{\mathrm{gal}}), \quad m = v_p(\mathrm{dis}\, E)$$

On s'intéresse à l'action de I sur $\underline{E}$. On sait que I s'injecte dans $\mathrm{Perm}(\underline{E})$.

Il nous faut introduire un tout dernier invariant ; c'est l'analogue de l'exposant m pour la **différente** de l'extension $E/\mathbb{Q}_p$, c'est à dire :

$$d = v_\pi(\mathfrak{D})$$

où π et $\mathfrak{D}$ sont respectivement une uniformisante de E et la différente de l'extension $E/\mathbb{Q}_p$. On sait que (c.f. [21], Chap III, §6, Proposition 13) :

$$m = fd\,; \qquad \text{si } p \nmid e \text{ alors } e = d+1\,; \qquad \text{si } p \mid e \text{ alors } e \leqslant d.$$

En utilisant uniquement ces trois dernières propriétés, nous allons pouvoir cerner les extensions $E/\mathbb{Q}_p$ telles que $1 \leqslant v_p(\mathrm{dis}(E/\mathbb{Q}_p)) \leqslant 3$ et déterminer, pour chacune d'entre elles, l'image de I dans $\mathrm{Perm}(\underline{E})$.

Petit tableau récapitulatif :

Rappels : $m = v_p(\mathrm{dis}(E))$, $d = v_\pi(\mathfrak{D})$.

<table>
<tr><td></td><td>$d=1$</td><td colspan="2">$d=2$</td><td colspan="3">$d=3$</td></tr>
<tr><td>$m=1$</td><td>$f=1$
$e=2$
$n=2$
$p\neq 2$
$I=S_2$</td><td colspan="2">Impossible</td><td colspan="3">Impossible</td></tr>
<tr><td rowspan="2">$m=2$</td><td rowspan="2">$f=2$
$e=2$
$n=4$
$p\neq 2$
$I=\left\langle \begin{smallmatrix}\text{double}\\ \text{transposition}\end{smallmatrix}\right\rangle$</td><td colspan="2">$f=1$</td><td colspan="3" rowspan="2">Impossible</td></tr>
<tr><td>$e=3$
$n=3$
$p\neq 3$
$I=A_3$</td><td>$e=2$
$n=2$
$p=2$
$I=S_2$</td></tr>
<tr><td rowspan="2">$m=3$</td><td rowspan="2">$f=3$
$e=2$
$n=6$
$p\neq 2$
$I=\left\langle \begin{smallmatrix}\text{triple}\\ \text{transposition}\end{smallmatrix}\right\rangle$</td><td colspan="2" rowspan="2">Impossible</td><td colspan="3">$f=1$</td></tr>
<tr><td>$e=4$
$n=4$
$p\neq 2$
$I=C_4$</td><td>$e=2$
$n=2$
$p=2$
$I=S_2$</td><td>$e=3$
$n=3$
$p=3$
$I=S_3$</td></tr>
</table>

Commentaires :

Les renseignements de ce tableau concernant les quantités f, e, n et p s'obtiennent directement en utilisant les trois propriétés rappelées ci-avant (pour chaque case, on distingue les cas $p \mid e$ et $p \nmid e$). En revanche, pour mieux cerner le groupe d'inertie, en plus du critère de Van der Waerden-Dedekind, nous avons utilisé deux autres résultats, à savoir :

• Le groupe Γ est constitué de permutations paires de $\mathrm{Perm}(\underline{E})$ si et seulement si $\mathrm{dis}(E)$ est un carré ; en effet, fixons $(x_1, \ldots, x_n)$ une $\mathbb{Q}_p$-base E et notons $\tau_1, \ldots, \tau_n$ les n éléments de $\underline{E}$. On pose :

$$\delta = \det(\tau_j(x_i))_{i,j} \in E^{\mathrm{gal}}$$

Alors pour tout $\sigma \in \Gamma$, notant $\varepsilon(\sigma)$ la signature de σ (vu comme un élément de $\mathrm{Perm}(\underline{E})$), on a $\sigma(\delta) = \varepsilon(\sigma)\delta$ (σ ne fait que permuter les colonnes de la matrice $(\tau_j(x_i))_{i,j}$. Ainsi, comme $\mathrm{dis}(E) = \delta^2$ (au carré d'un inversible près), $\mathrm{dis}(E)$ est un carré si et seulement si $\delta \in \mathbb{Q}_p$ si et seulement si $\varepsilon(\sigma) = 1$ quelque soit $\sigma \in \Gamma$.

Remarque – Le côté local des objets manipulés n'a été d'aucune utilité dans la preuve précédente. On peut retranscrire cette démonstration dans un cadre des corps de caractéristique distincte de 2.

• Soit L un corps de nombres p-adiques galoisien ; notons $\mathcal{O}_L$ l'anneau des entiers de L, $\mathfrak{P}$ l'idéal maximal de L, et introduisons :

$$I_i = \{\sigma \in \Gamma \mid \forall x \in \mathcal{O}_L,\ \sigma(x) \equiv x \mod \mathfrak{P}^{i+1}\} \quad i = 0, 1$$

alors I_0 et I_1 sont deux sous-groupes du groupe d'inertie I. En fait, $I = I_0$. De plus, I_1 est un sous-groupe caractéristique de I, c'est un p-groupe et I/I_1 est un groupe cyclique d'ordre premier à p.

Remarque – Ces résultats constituent les prémices de l'étude des groupes de ramification. Notamment, je n'ai défini ici que I_0 et I_1, mais la définition donnée s'étend aux entiers $i \geqslant 0$ (c.f. [21], Chap 4, §1 ou [17], Chap 5, §2).

En outre, j'utiliserais que (c.f. [21] Corollaire 4, Chap 4, §2) :

$$I \simeq I_1 \rtimes I/I_1 \simeq p\text{-groupe} \rtimes \begin{array}{c}\text{groupe cyclique}\\ \text{d'ordre premier à } p\end{array}$$

chacun de ces deux sous-groupes pouvant bien sûr être trivial. En particlulier le sous-groupe I_1 est réduit à l'identité si et seulement si l'extension $L/\mathbb{Q}_p$ est modérément ramifiée (i.e. $e(L/\mathbb{Q}_p)$ premier avec p). En conséquence, le groupe d'inertie d'une extension **modérément ramifiée** est cyclique.

Remarque – Bien qu'énoncés dans le cadre des corps de nombres p-adiques, ces résultats restent valables dans le cadre des extensions (finies) de corps locaux pour peu que les extensions résiduelles soient **séparables**. Dans l'étude que J.P Serre fait des groupes de ramifications (c.f. [21], Chap IV), il suppose cette hypothèse réalisée.

Cela étant, procédons ligne par ligne, la première ne posant aucun problème :

• Dans les cases (2-1) et (2-2, colonne 1), en appliquant le critère de Van der Waerden-Dedekind, on obtient, respectivement, les injections $I \hookrightarrow S_2 \times S_2$ et $I \hookrightarrow S_3$. Mais dans les deux cas, l'extension considérée, est modérément ramifiée. Par suite, les groupes d'inertie en question sont cycliques, d'où les précisions avancées.

• Réglons pour commencer le cas des extensions modérément ramifiées de la troisième ligne, à savoir les cases (3-1) et (3-3, colonne 1). A priori, grâce au critère de Van der Waerden-Dedekind, on peut seulement affirmer que : $I \hookrightarrow S_2 \times S_2 \times S_2$ (3-1) et $I \hookrightarrow S_4$ (3-3, colonne 1). Dans la première case, tenant compte du fait que l'on est dans le cas modérément ramifié, le groupe d'inertie étant cyclique, il ne peut être qu'une triple transposition. Dans la deuxième case, en utilisant le même argument, on montre que I est un sous-groupe cyclique transitif de S_4 ; or les sous-groupes transitifs de S_4 sont (à conjugaison près) :

sous-groupes	S_4	A_4	D_4	C_4	$E(4) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$
ordres	24	12	8	4	4

Parmi ces derniers, seul C_4 est cyclique.

Enfin, dans la troisième colonne de la case (3-3), I est a priori un sous-groupe transitif de S_3, mais A_3 est exclu car le discriminant du corps E n'est pas un carré (une puissance impaire d'une uniformisante ne peut pas être un carré).

II.4.3 Propriétés des premiers de faible exposant dans le discriminant d'un corps de nombres

Dans cette section, aidés des résultats précédents, nous allons énoncer des propriétés relatives aux premiers ne figurant qu'avec un petit exposant dans le discriminant d'un corps de nombres. Commençons par étudier les premiers qui ne figurent qu'une seule fois dans le discriminant :

Proposition 21 *Soit K un corps de nombres et p un premier de $\mathbb{Z}$ tel que $v_p(\operatorname{dis} K) = 1$. Pour tout idéal premier $\mathfrak{P}$ de K^{gal} au dessus de p, le groupe d'inertie $I(\mathfrak{P})$ associé à $\mathfrak{P}$ est engendré par une transposition.*

Preuve — Compte tenu de l'égalité :

$$v_p(\operatorname{dis} K) = \sum_{\mathfrak{p} \in \operatorname{Spec}_p(K)} v_p(\operatorname{dis} K_{\mathfrak{p}})$$

il existe un unique premier $\mathfrak{p}$ de K (au dessus de p) tel que p soit ramifié dans $K_{\mathfrak{p}}$; de plus,

$$v_p(\operatorname{dis} K_{\mathfrak{p}}) = 1$$

Par suite, pour un quelconque premier, $\mathfrak{P}$, de K^{gal} au dessus de p, $I(\mathfrak{P})$, qui est **non trivial**, s'injecte, en vertu du diagramme 3, dans $I(K_{\mathfrak{p}}^{\mathrm{gal}}/\mathbb{Q}_p)$ (les groupes d'inertie $I(K_{\mathfrak{q}}^{\mathrm{gal}}/\mathbb{Q}_p)$ pour $\mathfrak{q} \in \operatorname{Spec}_p(K) \setminus \{\mathfrak{p}\}$ sont triviaux). Enfin, comme $v_p(\operatorname{dis} K_{\mathfrak{p}}) = 1$, d'après l'étude locale précédente, on a nécessairement :

$$I(K_{\mathfrak{p}}^{\mathrm{gal}}/\mathbb{Q}_p) = S_2$$

de sorte que $I(\mathfrak{P})$ est bien réduit à une transposition. □

Corollaire 3 *Soit $F \in \mathbb{Z}[X]$ un polynôme irréductible unitaire de degré **premier** p. Pour que le groupe de Galois de F (sur $\mathbb{Q}$) soit égal à S_p, il suffit que dans la décomposition primaire de son discriminant il y ait **un** premier d'exposant 1.*

Preuve — En appliquant le résultat précédent au corps de nombres K engendré par une racine de F, on déduit que le groupe de Galois de F contient une transposition ; or un sous-groupe transitif de S_p contenant une transposition ne peut être que S_p. □

Corollaire 4 *Soit K un corps de nombres de degré n. Si $\text{dis}(K)$ est sans facteur carré, alors le groupe de Galois (sur $\mathbb{Q}$) de la clôture galoisienne de K est égal à S_n.*

Preuve — D'après la proposition 21 tous les premiers ramifiés de K^{gal} ont un groupe d'inertie réduit à une transposition. Cela étant, on sait que le groupe de Galois $\text{Gal}(K^{\text{gal}}/\mathbb{Q})$ est engendré par ces groupes d'inertie ; or le seul sous-groupe transitif de S_n engendré par des transpositions est S_n. □

Bien sûr, on a le sous-produit polynomial de ce corollaire, à savoir :

Corollaire 5 *Soit $F \in \mathbb{Z}[X]$ un polynôme irréductible unitaire de degré n dont le discriminant est sans facteur carré, alors le groupe de Galois de F (sur $\mathbb{Q}$) est égal à S_n.*

Comme le suggère T.Kondo dans [12], on obtient un résultat analogue, en laissant un petit peu plus de lattitude à l'exposant du premier 2. Plus précisément, dans cet article, l'auteur étudie les corps de nombres dont le discriminant est égal au discriminant d'un corps quadratique. Rappelons, à ce propos, que pour $\Delta \in \mathbb{Z}$, on a l'équivalence :

$$\Delta \text{ est le discriminant d'un corps quadratique,} \quad \text{si et seulement si :} \quad \begin{cases} \Delta \text{ n'est pas un carré et} \\ \Delta = \text{dis}(\mathbb{Q}(\sqrt{\Delta})) \end{cases}$$

Par exemple, 20 n'est pas le discriminant d'un corps quadratique, car $\text{dis}(\mathbb{Q}(\sqrt{20})) = \text{dis}(\mathbb{Q}(\sqrt{5})) = 5$, alors que -20, lui, en est un car $\text{dis}(\mathbb{Q}(\sqrt{-20})) = \text{dis}(\mathbb{Q}(\sqrt{-5})) = -20$; en effet, étant donné $d \in \mathbb{Z}$ sans facteur carré (ce qui implique que $d \not\equiv 0 \pmod 4$), on sait que :

$$\text{dis}(\mathbb{Q}(\sqrt{d})) = \begin{cases} d & \text{si } d \equiv 1 \pmod 4 \\ 4d & \text{si } d \equiv 2, 3 \pmod 4 \end{cases}$$

Remarque – En particulier, le discriminant d'un corps quadratique est congru à 0 ou 1 modulo 4. En fait, plus généralement, nous avons le résultat :

Proposition 22 (Stickelberger) *Etant donnés K un corps de nombres de degré n et $(x_1, \ldots, x_n)$ une $\mathbb{Q}$-base de K formée d'éléments **entiers** sur $\mathbb{Z}$ alors :*

$$\text{dis}_{K/\mathbb{Q}}(x_1, \ldots, x_n) \equiv 0 \text{ ou } 1 \mod 4$$

Ainsi, pour tout corps de nombres K, il est impossible d'avoir $v_2(\text{dis}\, K) = 1$.

Enfin, comme le montre ce qui précède, nécessairement, la factorisation du discriminant Δ d'un corps quadratique est de la forme :

$$\pm 2^{0,\ 2 \text{ ou } 3} \times (\text{produit de premiers impairs distincts})$$

Par suite, si Δ est le discriminant d'un corps quadratique, alors $v_2(\Delta) \leqslant 3$; nous tiendrons compte de cette remarque dans le corollaire suivant :

Corollaire 6 *Soit K un corps de nombres de degré n. Si le discriminant de K est le discriminant d'un corps quadratique, alors le groupe de Galois (sur $\mathbb{Q}$) de la clôture galoisienne de K est égal à S_n.*

Preuve — D'après ce qui précède, tous les premiers impairs divisant $\text{dis}(K)$ ne figurent qu'une seule fois dans la factorisation de ce dernier ; par suite, d'après la proposition 21, tous les premiers de K^{gal} au dessus d'un premier impair de $\mathbb{Z}$ (ramifié dans K, i.e. divisant $\text{dis}(K)$) ont un groupe d'inertie réduit à une transposition. Il reste le cas des premier de K^{gal} au dessus de 2 (dans le cas où ce dernier est ramifié dans K bien entendu).

Remarquons, tout d'abord, que pour tout premier $\mathfrak{p}$ de K au dessus de 2, il est impossible d'avoir $v_2(\mathrm{dis}(K_\mathfrak{p}/\mathbb{Q}_2)) = 1$, comme le montre la première case du tableau récapitulatif précédent. Ensuite, nous venons de le noter, nécessairement, $v_2(\mathrm{dis}(K)) \leqslant 3$, par conséquent,

$$v_2(\mathrm{dis}(K_\mathfrak{p}/\mathbb{Q}_2)) \in \{2, 3\} \tag{4}$$

et une nouvelle fois, il n'y a qu'un seul premier, $\mathfrak{p}$ de K au dessus de 2 tel que 2 soit ramifié dans $K_\mathfrak{p}$. Le reste de la démonstration consiste à montrer que pour tout premier $\mathfrak{P}$ de K^{gal} au dessus de 2, $I(\mathfrak{P})$ est encore réduit à une transposition afin de pouvoir conclure avec le même type d'arguments que dans la preuve précédente.

Un nouvel examen du tableau récapitulatif, en tenant compte de (4), nous montre qu'il suffit d'écarter le cas où (case 2-2, colonne 1) :

$$e(K_\mathfrak{p}/\mathbb{Q}_2) = 3, \quad f(K_\mathfrak{p}/\mathbb{Q}_2) = 1 \quad \text{et} \quad I(= I(\mathfrak{P})) = A_3$$

Pour cela, nous allons faire opérer $\Gamma = \mathrm{Gal}(K^{\mathrm{gal}}/\mathbb{Q})$ sur $\underline{E}$, avec $E = \mathbb{Q}(\sqrt{\mathrm{dis}\,K})$ (l'extension $E/\mathbb{Q}$ est une sous-extension de l'extension $K^{\mathrm{gal}}/\mathbb{Q}$). Le premier 2 étant ramifié dans E (car $\mathrm{dis}(K)$ est le discriminant d'un corps quadratique donc $\mathrm{dis}(K) = \mathrm{dis}(E)$), d'après le critère de Van der Waerden-Dedekind, $I = I(\mathfrak{P})$ opère transitivement sur un ensemble à deux éléments ; en conséquence, on ne peut pas avoir $I(\mathfrak{P}) = A_3$ et il ne reste plus que l'alternative $I(\mathfrak{P}) = S_2$. $\square$

II.5 Quand l'indice de ramification et la caractéristique du corps résiduel sont premiers entre eux

Une autre illustration du théorème de Van der Waerden-Dedekind consiste à étudier pour un corps de nombres K donné, les premiers p de $\mathbb{Z}$ tels que l'indice de ramification de tout premier $\mathfrak{p}$ de K (au dessus de p) est premier avec p.

Proposition 23 *Soit K un corps de nombres et p un premier de $\mathbb{Z}$ tel que :*

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g} \qquad \textit{avec} \quad e_i \wedge p = 1 \quad \textit{et} \quad N_{K/\mathbb{Q}}(\mathfrak{p}_i) = p^{f_i}$$

Alors pour tout premier $\mathfrak{P}$ de K^{gal} au dessus de p, le groupe d'inertie $I(\mathfrak{P})$ est cyclique ; de plus, tout générateur σ de $I(\mathfrak{P})$ (vu comme permutation de $\underline{K}$) a une décomposition en cycles (à supports disjoints) de la forme :

$$\sigma = (\underbrace{(lg.\ e_1)\cdots(lg.\ e_1)}_{f_1\ cycles})\cdots(\underbrace{(lg.\ e_g)\cdots(lg.\ e_g)}_{f_g\ cycles})$$

Preuve — Notons $L = K^{\mathrm{gal}}$ et considérons $\mathfrak{P}$ un premier de L au dessus de p. Commençons par vérifier que l'extension $L_\mathfrak{P}/\mathbb{Q}_p$ est modérément ramifiée. Tout d'abord, pour tout premier $\mathfrak{p}$ de K au dessus de p, l'extension $K_\mathfrak{p}/\mathbb{Q}_p$ est, bien sûr, modérément ramifiée ; par suite, reprenant les notations de la section II.4.1, il en est de même de l'extension $K_\mathfrak{p}^{\mathrm{gal}}/\mathbb{Q}_p$, car c'est le compositum d'extensions modérément ramifiées (c.f. [13], Chap 2, §5 ou [17], Chap 5, §2, n°2). Mais comme $L = K^{\mathrm{gal}}$, nous l'avons déja remarqué (toujours dans la section II.4.1), $L_\mathfrak{P}$ n'est rien d'autre que le compositum des $K_\mathfrak{p}^{\mathrm{gal}}$, l'idéal $\mathfrak{p}$ décrivant l'ensemble $\mathrm{Spec}_p(K)$; le même argument que précédemment montre que l'extension $L_\mathfrak{P}/\mathbb{Q}_p$ est modérément ramifiée.

En conséquence, $I(\mathfrak{P}) = I(L_\mathfrak{P}/\mathbb{Q}_p)$ est un groupe cyclique. On note σ un de ses générateurs et on fait opérer ce dernier sur $\underline{K}$. D'après le critère de Van der Waerden-Dedekind, σ décompose $\underline{K}$ en f_1 orbites de longueur e_1, f_2 orbites de longueur e_2, etc... On conclut en utilisant le fait que les orbites d'un groupe cyclique agissant **fidèlement** sur un ensemble, correspondent à la décomposition en cycles à supports disjoints d'un générateur de ce groupe. $\square$

De plus, on va montrer qu'aucun premier de K au dessus de p n'est ramifié dans $L = K^{\mathrm{gal}}$.

Remarque – Si tous les premiers ramifiés d'un corps de nombres K vérifient les hypothèses de la proposition précédente, aucun premier de K n'est ramifié dans K^{gal}. Cette situation n'est pas banale ; en effet une telle situation est exclue si le corps de base (i.e. K) est $\mathbb{Q}$, comme le montre le théorème suivant (c.f. [20], Chap IV, §3, Théorème 1) :

Théorème 6 (Hermite-Minkowski) *Pour tout corps de nombres K, distinct de $\mathbb{Q}$, le discriminant de K sur $\mathbb{Q}$, $\mathrm{dis}(K)$, est différent de ± 1.*

Autrement dit, dans tout corps de nombres (distinct de $\mathbb{Q}$), il y a un premier de $\mathbb{Q}$ qui se ramifie.

Soit $\mathfrak{P}$ un premier de L ; on note $\mathfrak{p}$ le premier de K que couvre $\mathfrak{P}$. Le but de ce qui suit est de montrer que $e(\mathfrak{P}/K) = 1$, ce qui revient à montrer, en vertu de la multiplicativité des indices de ramifications, que $e(\mathfrak{P}/\mathbb{Q}) = e(\mathfrak{p}/\mathbb{Q})$. Localisons, en indiquant les indices de ramifications qui nous intéressent :

$$\begin{tikzcd}[column sep=small]
L_{\mathfrak{P}} \arrow[dd, dash, "e(L_{\mathfrak{P}}/\mathbb{Q}_p)"'] \arrow[dr, dash, "e(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \overset{?}{=} 1"] & \\
& K_{\mathfrak{p}} \arrow[dl, dash, "e(K_{\mathfrak{p}}/\mathbb{Q}_p)"] \\
\mathbb{Q}_p &
\end{tikzcd}
\qquad \text{avec : } \begin{cases} e(L_{\mathfrak{P}}/\mathbb{Q}_p) = e(\mathfrak{P}/\mathbb{Q}) \\ e(K_{\mathfrak{p}}/\mathbb{Q}_p) = e(\mathfrak{p}/\mathbb{Q}) \\ e(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = e(\mathfrak{P}/K) \end{cases}$$

Comme le compositum d'extensions non ramifiées est non ramifiée (c.f. [13], Chap 2, §4 ou [17], Chap 5, §2, n°1), il suffit en fait de montrer que pour tout premier $\mathfrak{p}$ de K au dessus de p, l'extension $K_{\mathfrak{p}}^{\text{gal}}/K_{\mathfrak{p}}$ est non ramifiée. On est donc ramené à la situation locale suivante, en posant $E = K_{\mathfrak{p}}$:

$$\begin{tikzcd}[column sep=small]
E^{\text{gal}} \arrow[dd, dash] \arrow[dr, dash, "e(E^{\text{gal}}/E) \overset{?}{=} 1"] & \\
& E \arrow[dl, dash] \\
\mathbb{Q}_p &
\end{tikzcd}
\qquad \text{où l'extension } E/\mathbb{Q}_p \text{ est modérément ramifiée, donc } E^{\text{gal}}/\mathbb{Q}_p \text{ aussi}$$

Une nouvelle fois, $I(E^{\text{gal}}/\mathbb{Q}_p)$ est cyclique ; notons σ un générateur. Considéré comme une permutation de $\underline{E}$ ce dernier décompose, d'après le critère de Van der Waerden-Dedekind, $\underline{E}$ en $f(E/\mathbb{Q}_p)$ orbites, toutes de longueur $e(E/\mathbb{Q}_p)$. Par suite σ est d'ordre $e(E/\mathbb{Q}_p)$; il en est donc de même de $I(E^{\text{gal}}/\mathbb{Q}_p)$ (puisque σ engendre ce sous-groupe). Il suffit maintenant de se souvenir que $I(E^{\text{gal}}/\mathbb{Q}_p)$ est aussi le groupe de Galois de l'extension $E^{\text{gal}}/E_0^{\text{gal}}$ (où E_0^{gal} est la plus grande extension de $\mathbb{Q}_p$ non ramifiée contenue dans E^{gal}), qui est justement de degré $e(E^{\text{gal}}/\mathbb{Q}_p)$; ainsi $e(E^{\text{gal}}/\mathbb{Q}_p) = e(E/\mathbb{Q}_p)$, d'où la conclusion.

Remarque – En fait cette propriété est une conséquence d'un résultat général de la théorie des corps locaux, à savoir (c.f. [17], Chap 5, §2, n°3) :

Lemme 6 (Abhyankar) *Si L/K est une extension modérément ramifiée de corps locaux et M/K une autre extension finie dont l'indice de ramification est un multiple de celui de L/K, alors l'extension ML/M est non ramifiée.*

Un excellent exercice consiste à retrouver ce que nous venons d'établir en utilisant ce lemme.

II.6 Le critère de Van der Waerden-Dedekind dans les corps munis de valuations discrètes

Quittons maintenant le cadre des corps de nombres. En se cantonnant à ce dernier, on acquiert certains réflexes qu'il convient de contrôler dans un cadre plus général. Par exemple, le sous-anneau $\mathbb{Z}$ a un statut ultra-privilégié. Il porte, en particulier, toutes les valuations non triviales sur le corps $\mathbb{Q}$ (ou de manière équivalente il est contenu dans tous les anneaux de valuation pour $\mathbb{Q}$). Dans le même ordre d'idée, l'anneau $\mathbb{Z}$ induit (par fermeture intégrale) un sous-anneau privilégié de tout corps de nombres K, à savoir son anneau d'entiers. Cet anneau porte lui aussi toutes les valuations du corps K. L'intérêt du langage des valuations est alors un tant soit peu "gommé" dans les corps de nombres.

En revanche, dans le cadre des corps K des fonctions algébriques sur un corps k (en particulier, les extensions pures de degré de transcendance 1 de k) aucun sous-anneau ne joue le rôle que peut avoir $\mathbb{Z}$ pour $\mathbb{Q}$. En effet, nous avons déjà constaté que pour décrire toutes les valuations d'une extension pure de degré de transcendance 1, il faut, une fois choisi un générateur x de K/k, considérer les sous-anneaux $k[x]$ et $k[x^{-1}]$. Dès lors, la puissance des raisonnements "valuationnels" est beaucoup plus significative dans ce type de corps.

En bref, nous allons plus ou moins changer notre discours dans cette section. Il ne sera plus question d'idéal premier $\mathfrak{p}$ du corps[9] K mais de valuation sur K. Si K est muni d'une valuation v discrète, alors cette dernière admet un nombre fini de prolongements à toute extension L finie de K. Pour chaque prolongement w,

[9] Notons à ce propos que, déjà, on oubiait l'anneau sous-jacent. Cet abus de langage n'est évidemment pas un hasard ; l'idéal $\mathfrak{p}$ masque en fait une valuation sur le corps K.

on définit les quantités $e(w/K)$ et $f(w/K)$ qui sont respectivement l'indice de ramification et le degré résiduel[10]. Si v admet g prolongements, $w_1, \dots, w_g$ à L, on écrit pour être concis :

$$v = w_1^{e_1} \cdots w_g^{e_g} \qquad \text{avec} \qquad f(w_i/K) = f_i$$

De la même manière, si l'extension L/K est de plus galoisienne de groupe de Galois Γ, alors nous verrons apparaître les sous-groupes de décomposition et d'inertie $D(w/K)$ et $I(w/K)$ définis par :

$$D(w/K) = \mathrm{Gal}(L_w/K_v) \qquad \text{et} \qquad I(w/K) = I(L_w/K_v)$$

où K_v et L_w désignent les complétés respectifs de K et L pour v et w (ce sont bien évidemment des corps locaux si les valuations considérées sont discrètes).

Quand j'ai commencé à comprendre le critère de Van der Waerden-Dedekind de la théorie des nombres, je me suis posé la question de savoir s'il existait un cadre plus général pour cet énoncé. En l'absence de références, et trouvant déjà quelques satisfactions à appliquer ce critère dans le cadre des corps de nombres, je laissais momentanément cette question en suspend ; jusqu'au jour où Claude Quitté me mit, entre les mains, un exemplaire du préprint co-écrit par Malle et Matzat (c.f. [15]). Dans cet ouvrage (Chap 1 §9.1), figure, en effet, un énoncé général du si bien nommé critère de Van der Waerden-Dedekind que je retranscris ici :

Théorème 7 *Soit K un corps muni d'une valuation discrète v, E/K une extension finie et séparable de K et enfin L/K une extension galoisienne de K contenant E. On considère w un prolongement de v au corps L tel que l'extension l/k des corps résiduels soit séparable. Désignons par $D(w/K)$ le groupe de décomposition de w sur K (i.e. $\mathrm{Gal}(L_w/K_v)$) et $I(w/K)$ le groupe d'inertie de w sur K (i.e. $I(L_w/K_v)$). Si v se prolonge au corps E en $v_1, \dots, v_g$ avec :*

$$v = v_1^{e_1} \cdots v_g^{e_g} \qquad \textit{et} \qquad f(v_i/K) = f_i$$

alors $D(w/K)$ décompose $\underline{E} = \mathrm{Hom}_K(E, L)$ en g orbites de longueur respective $e_i f_i$ et chacune d'entre elles se décompose en f_i $I(w/K)$-orbites de longueurs e_i.

La preuve de cette généralisation est bien évidemment sensiblement identique à celle faite dans le cadre des corps de nombres. Cependant, suivant Malle et Matzat, toujours dans [15], il est possible d'en simplifier sensiblement la deuxième partie en remarquant que nous ne cherchons que le **cardinal** d'une quelconque $I(w/K)$-orbite (on sait qu'elles ont toutes le même cardinal) et non l'orbite elle même !

Preuve — Pour le calcul du cardinal des $D(w/K)$-orbites de $\underline{E}$, on procède comme dans le cadre des corps de nombres. On remarque que :

$$\underline{E} = \bigvee_{i=1}^{g} \{\sigma \in \underline{E},\ w \circ \sigma = v_i\}$$

Et pour chaque $1 \leqslant i \leqslant g$, on a un isomorphisme canonique (la restriction) entre :

$$\{\sigma \in \underline{E},\ w \circ \sigma = v_i\} \simeq \mathrm{Hom}_{K_v}(E_i, L_w)$$

où K_v, E_i et L_w désignent les complétés respectifs des corps K, E et L pour les valuations v, v_i et w. De plus l'extension L_w/K_v est galoisienne de groupe de Galois canoniquement isomorphe à $D(w/K)$. Ainsi, à chaque prolongement v_i de la valuation v à E est associé une $D(w/K)$-orbite dont le cardinal n'est rien d'autre que celui de $\mathrm{Hom}_{K_v}(E_i, L_w)$, à savoir $e_i f_i$.

En complétant, on ramène, pour le calcul du cardinal d'une $I(w/K)$-orbite de $\underline{E}$ à l'étude de la situation locale :

$$\begin{tikzcd} L \arrow[dd, dash, "\Gamma"'] \arrow[dr, dash] & \\ & E \arrow[dl, dash] \\ K & \end{tikzcd} \qquad \text{(Situation locale)}$$

où, par hypothèse :

[10]Dans le cadre des valuations discrètes, on retrouve, en revenant aux anneaux de valuation sous-jacents et leurs idéaux maximaux respectifs les définitions usuelles des quantités e et f. On peut cependant définir des quantités "analogues" pour des valuations quelconques (c.f. l'annexe A).

- K, E et L sont des corps locaux ;
- l'extension L/K est galoisienne de groupe de Galois Γ ;
- l'extension l/k des corps résiduels respectifs de L et K est **séparable**.

On cherche le cardinal d'une $I(L/K)$-orbite. Grâce au lemme 4, on peut se contenter de calculer l'orbite de l'injection canonique $i \in \underline{E}$. Ce dernier est égal à :

$$\#I.i = \frac{\#I}{\#\operatorname{Stab}_I(i)} \qquad \text{où on a posé } I = I(L/K)$$

Puisque l'extension résiduelle l/k a été supposée séparable, cette extension est en fait galoisienne ; ainsi, $\#I = e(L/K)$. Il reste à déterminer le cardinal de $\operatorname{Stab}_I(i)$. Pour cela, il suffit de remarquer que (c.f. [21], Chap I, §7, Proposition 22) :

$$\operatorname{Stab}_I(i) = I \cap \operatorname{Stab}_{\operatorname{Gal}(L/E)}(i) = I \cap \operatorname{Gal}(L/E) = I(L/E)$$

Comme $\#I(L/E) = e(L/E)$, en utilisant la formule de transitivité des indices de ramification, on montre bien que : $\#I.i = e(E/K)$, ce que l'on voulait. $\square$

II.7 Exemples dans les extensions pures de degré de transcendance 1

II.7.1 Les valuations des corps de fractions rationnelles

Soit k un corps (commutatif !) et K une extension pure de degré de transcendance 1 sur k ; c'est à dire, une fois choisi un générateur x de K/k, le corps des fractions rationnelles $K = k(x)$. Rappelons qu'il est possible de décrire l'ensemble, $\operatorname{Spec}(K)$, de toutes les valuations sur K triviales sur k :

$$\operatorname{Spec}(K) = \{v_{x,\pi},\ \pi \text{ irréductible unitaire de } k[x]\} \cup \{v_{x,\infty}\}$$

Cette description est à l'évidence intimement liée au choix préalable du générateur x de K/k.

Pour chaque valuation v, on appelle degré de v et on note $\deg(v)$, la quantité $\dim_k(V/\mathfrak{m}(V))$ où V est l'anneau de valuation pour K associé à v et $\mathfrak{m}(V)$ son idéal maximal. Bien sûr, si $v = v_{x,\pi}$, avec π un irréductible de $k[x]$, on a : $\deg(v) = \deg(\pi)$. Nous nous attarderons plus particulièrement sur les valuations de degré 1, dont on note l'ensemble $\operatorname{Spec}_1(K)$. Ce dernier est, en vertu de ce qui précède, en bijection avec $\mathbb{P}_1(k)$.

Remarque – Si le corps de base k est algébriquement clos, toutes les valuations sur K sont de degré 1.

Autour du théorème de Luröth :

Considérons maintenant L une extension pure de degré de transcendance 1 sur k, c'est-à-dire, une fois choisi x un générateur, le corps $L = k(x)$. Soit R une fraction rationnelle de $k(x)$, on peut considérer l'extension $k(x)/k(R(x))$; si $\operatorname{ht}(R)$ désigne la hauteur de la fraction rationnelle R (i.e. $\operatorname{ht}(R) = \max\{\deg f, \deg g\}$ où $R = f/g$ avec $f, g \in k[x]$ premiers entre eux) alors l'extension $k(x)/k(R(x))$ est finie de degré $\operatorname{ht}(R)$. Nous abuserons de ce procédé de construction dans toute la suite de cette section. En particulier, si $f \in k[T]$ est un polynôme de degré n, on peut considérer l'extension (de degré n) : $k(x)/k(y)$ où $y = f(x)$. Le polynôme minimal de x sur $k(y)$ est bien sûr, à un scalaire près le polynôme $f(T) - y \in k(y)[T]$.

Cela étant, afin de pouvoir appliquer à ce cadre, le critère de Van der Waerden-Dedekind, il est est bon de revoir les questions de prolongements et de ramification en utilisant la description des valuations. Le cadre est bien évidemment le suivant : soit L un corps de fractions rationnelles sur k (un corps quelconque pour l'instant) dont on note x un générateur, i.e. $L = k(x)$; si $R \in k(x)$ est une fraction rationnelle non constante alors on introduit $K = k(R(x))$ le sous corps de L, de sorte que :

$$k \overset{\text{transcendant}}{\overline{\qquad\qquad\qquad}} K = k(y) \overset{n}{\overline{\qquad\qquad\qquad}} L = k(x) \qquad \text{avec} \qquad y = R(x) \quad n = \operatorname{ht}(R)$$

Si dans le cadre des corps de nombres le point de départ était souvent une valuation sur $\mathbb{Q}$ que l'on prolongeait de toutes les manières possibles, il est souvent plus commode ici de se fixer une valuation w sur L et d'étudier sa restriction v à K. A cet effet, il nous faut introduire pour $R \in k(x)$ une application de $\mathbb{P}_1(k)$ dans lui même associée à R. Posons $R = f/g$ où f et g sont deux polynômes de $k[x]$ premiers entre eux et notons

n la hauteur de R. On introduit $\widetilde{f}$ et $\widetilde{g} \in k[U,V]$ les homogénéisés en degré n (à deux variables) de f et g respectivement, c'est à dire :

$$\widetilde{f}(U,V) = V^n f(U/V) \qquad \text{et} \qquad \widetilde{g}(U,V) = V^n g(U/V)$$

On obtient ainsi, deux polynômes homogènes de degré n en U et V, qui sont premiers entre eux dans $k[U,V]$ dès que f et g le sont dans $k[x]$ (car n est exactement la hauteur de R). Par conséquent, on peut définir l'application suivante :

$$\begin{array}{ccc} k^2 \setminus \{0\} & \longrightarrow & k^2 \setminus \{0\} \\ (u,v) & \longmapsto & (\widetilde{f}(u,v), \widetilde{g}(u,v)) \end{array}$$

Cette application étant, on le vérifie facilement, compatible avec la relation d'équivalence projective, elle définit, par passage au quotient, une application de $\mathbb{P}_1(k)$ dans lui même ; on la note $R^{\#}$.

Remarque – Pour ce qui est de l'utilisation de la fonction $R^{\#}$ dans la suite[11], on peut garder à l'esprit une définition naïve qu'il est possible de donner, à savoir :

$$\forall \lambda \in \mathbb{P}_1(k), \qquad R^{\#}(\lambda) = \begin{cases} R(\lambda) & \text{si } \lambda \in k \text{ et si } R \text{ est définie en } \lambda \\ \infty & \text{si } \lambda \in k \text{ est un pôle de } R \\ a/b & \text{si } \lambda = \infty, \deg(R) = 0 \text{ et } R = \frac{aX^n + \cdots}{bX^n + \cdots} \\ \infty & \text{si } \lambda = \infty \text{ et si } \deg(R) > 0 \\ 0 & \text{si } \lambda = \infty \text{ et si } \deg(R) < 0 \end{cases}$$

Montrons maintenant la formule :

Proposition 24 *Sous les hypothèses précédentes, on considère $w \in \mathrm{Spec}_1(k)$ et $\lambda \in \mathbb{P}_1(L)$ tel que $w = w_{x,\lambda}$; notons v la restriction de w à K, alors v est elle aussi de degré 1, i.e. $v \in \mathrm{Spec}_1(K)$. De plus v s'exprime de la manière suivante :*

- *si $R^{\#}(\lambda) \in k$ alors :*
$$v(\bullet) = w_{x,\lambda}\left(R(x) - R^{\#}(\lambda)\right) \times v_{y,R^{\#}(\lambda)}(\bullet)$$
- *si $R^{\#}(\lambda) = \infty$ alors :*
$$v(\bullet) = w_{x,\lambda}\left(\frac{1}{R(x)}\right) \times v_{y,R^{\#}(\lambda)}(\bullet)$$

Preuve — Tout d'abord, remarquons que :

$$\deg(w) = f(w/K) \times \deg(v) \ ;$$

par conséquent, si $\deg(w) = 1$, alors il en est de même du degré de la restriction de w à K ; autrement dit $\deg(v) = 1$. Pour le reste, puisque les valuations manipulées sont discrètes, il suffit de s'assurer que les égalités avancées sont valides pour une uniformisante de $v_{y,R^{\#}(\lambda)}$. C'est immédiat en choisissant, dans le premier cas $y - R^{\#}(\lambda)$ et dans le second $1/y$. □

Proposition 25 *Soit k un corps* ***de caractéristique nulle*** *et $L = k(x)$ un corps de fractions rationnelles sur k. On considère un polynôme $f \in k[T]$ de degré n ainsi que la tour d'extensions associée :*

$$\underbrace{k \qquad\qquad K}_{\textit{transcendant}} = \underbrace{k(y) \qquad\qquad L}_{n} = k(x) \qquad \textit{avec} \qquad y = f(x)$$

Alors :

1. *la valuation à l'infini, c'est-à-dire $w_{x,\infty}$, définie sur L est totalement ramifiée sur K ; autrement dit, $e(w_{x,\infty}/K) = n$ et $f(w_{x,\infty}/K) = 1$;*
2. *les seules autres valuations de L qui sont ramifiées sur K sont exactements les valuations de la forme $w_{x,\pi}$ où π est un diviseur irréductible de f' (la dérivée du polynôme f en T) ; plus précisément, si f' se factorise sous la forme :*
$$f'(T) = \pi_1^{e'_1}(T) \cdots \pi_g^{e'_g}(T)$$
alors pour tout $1 \leqslant i \leqslant g$, on a :
$$e(w_i/K) = e'_i + 1$$
où on a noté, $w_i = w_{x,\pi_i}$.

[11] L'utilisation de l'application $R^{\#}$ ne sera que purement descriptive.

Cette proposition est un cas particulier d'un résultat beaucoup plus général faisant intervenir la différente de l'extension L/K (c.f. [21], Chap III, §6, Proposition 13). Nous donnons une preuve élémentaire qui utilise la "description des valuations".

Preuve dans le cas où le corps k est algébriquement clos — En vertu de la proposition 24, on sait que :

$$w_{x,\infty|K}(\bullet) = w_{x,\infty}\left(\frac{1}{f(x)}\right) \times v_{f(x),\infty}(\bullet) = -\deg\left(\frac{1}{f(x)}\right) \times v_{f(x),\infty}(\bullet) = n \times v_{f(x),\infty}(\bullet)$$

ce qui montre bien que $e(w/K) = n$, ou encore que w est totalement ramifié sur K.

Pour le deuxième point, nous nous contentons de nous placer au dessus d'un corps algébriquement clos où toutes les valuations sont de degré 1. Tout est prêt pour conclure sous cette hypothèse. En effet, soit $w \in \mathrm{Spec}_1(L) \setminus \{w_{x,\infty}\}$; on écrit $w = w_{x,\lambda}$ (avec $\lambda \in k$). En vertu de la proposition 24, la valuation w est ramifiée sur K si et seulement si :

$$w_{x,\lambda}(f(x) - f(\lambda)) \geqslant 2$$

Autrement dit, nous cherchons les éléments $\lambda \in k$ tels que λ soit racine au moins double du polynôme $f(x) - f(\lambda)$. Nécessairement, λ est donc racine de f' ; la réciproque est immédiate d'où le résultat. □

Remarque – Le premier point admet un énoncé réciproque à savoir : pour que la valuation à l'infini, i.e. $w_{x,\infty}$ soit totalement ramifiée sur $k(R(x))$ (où R est une fraction rationnelle non constante), il faut et il suffit que R soit un polynôme en x.

Ces petits résultats suffiront à notre modeste objectif qui est, je le rappelle, d'illustrer le critère de Van der Waerden-Dedekind dans un cadre différent de celui des corps de nombres. La fin de cette section est consacrée à des exemples dans les extensions pures de degré de transcencance 1 d'un corps k de caractéristique nulle ou non.

II.7.2 Des exemples en caractéristique nulle

Dans le cadre des corps de nombres, l'examen du comportement des premiers (où des valuations) ramifiés n'est pas toujours très probant d'un point de vue pratique. Souvent, la factorisation modulo quelques premiers non ramifiés s'avère beaucoup plus fructueuse. La finitude des corps résiduels, qui entraîne le caractère cyclique des extensions résiduelles, est la principale explication de cette "injustice". Illustrons ce sombre propos : considérons le polynôme $F(T) = T^7 + 7T^4 + 14T + 3$. Il est irréductible dans $\mathbb{Z}[T]$ et son discriminant, $\mathrm{dis}(F) = 3^6 7^8$, est un carré ; par conséquent, son groupe de Galois sur $\mathbb{Q}$, $\mathrm{Gal}(F/\mathbb{Q})$, est un sous-groupe transitif de A_7 ; ces derniers sont au nombre de 4 (à conjugaison près) :

sous-groupes	$T(\mathbb{F}_7)$	$\subset$	$ASL_1(\mathbb{F}_7)$	$\subset$	$AGL_1(\mathbb{F}_7)$	$\subset$	A_7
ordres	7		3×7		$2^3 \times 3 \times 7$		$2^3 \times 3^2 \times 5 \times 7$

La factorisation de F modulo 5 et la forme "faible" du critère de Van der Waerden-Dedekind, nous permettent de montrer directement que $\mathrm{Gal}(F/\mathbb{Q}) = A_7$; en effet, on a :

$$F \equiv \text{(facteur de degré 5)(facteur de degré 1)(facteur de degré 1)} \mod 5,$$

par suite $\mathrm{Gal}(F/\mathbb{Q})$ contient un 5-cycle (d'ordre 5), or parmi les groupes énumérés, seul A_7 a un ordre divisible par 5. Que peut-on espérer de plus expéditif ?

Remarque – En plus, dans cet exemple, les factorisations des deux premiers ramifiés ne permettent pas facilement de donner le goupe de Galois. En effet, on peut vérifier que $\langle 3 \rangle = \mathfrak{p}^3\mathfrak{q}$ avec $f_\mathfrak{p} = 2$, $f_\mathfrak{q} = 1$ et $\langle 7 \rangle = \mathfrak{r}^7$ avec évidemment $f_\mathfrak{r} = 1$. La première factorisation montre que pour tout premier $\mathfrak{P}$ de K^{gal} au-dessus de 3 (où K est le corps de nombres engendré par une racine de F), $I(\mathfrak{P})$ s'injecte dans $S_3 \times S_3$ et est constitué de permutations paires ; quant à la seconde factorisation, elle montre que pour tout premier $\mathfrak{Q}$ de K^{gal} au dessus de 7, $I(\mathfrak{Q})$ est engendré par un 7-cycle...

En revanche, en caractéristique résiduelle nulle, par exemple au dessus de $\mathbb{Q}(T)$, le groupe de Galois des extensions résiduelles n'a plus aucune raison d'être cyclique. Il peut même être très compliqué. Dans ce contexte, l'examen des valuations ramifiées et plus particulièrement des groupes d'inertie, s'avère être beaucoup plus fructueux. En plus, en caractéristique résiduelle nulle, les extensions locales (obtenues en localisant et complétant) sont toutes **modérément** ramifiées (si ramifiées bien sûr). Par suite, les groupes d'inertie sont **cycliques**. Comme nous avons déduit, du critère de Van der Waerden-Dedekind pour les corps de nombres, la proposition 23, nous pouvons, à partir du théorème 7, montrer que :

Proposition 26 *Soit K un corps muni d'une valuation discrète v à corps résiduel de caractéristique nulle, E/K une extension finie et séparable de K et enfin $L = E^{gal}$ la clôture galoisienne de E sur K. On suppose que v se prolonge au corps E en $v_1, \ldots, v_g$ avec :*

$$v = v_1^{e_1} \cdots v_g^{e_g} \qquad \textit{et} \qquad f(v_i/K) = f_i$$

Alors, pour tout prolongement w de v au corps L le groupe d'inertie $I(w/K)$ est cyclique ; de plus, tout générateur σ de $I(w/K)$ (vu comme permutation de $\underline{E}$) a une décomposition en cycles (à supports disjoints) de la forme :

$$\sigma = \underbrace{((lg.\ e_1)\cdots(lg.\ e_1))}_{f_1\ cycles} \cdots \underbrace{((lg.\ e_g)\cdots(lg.\ e_g))}_{f_g\ cycles}$$

Remarque – Cette proposition est encore valide en caractéristique p si on suppose de plus que l'extension de corps résiduels l/k est séparable et si tous les e_i sont premiers avec p.

Traitons maintenant quelques exemples ; considérons les polynômes $F_n \in \mathbb{Q}(y)[T]$ définis par :

$$F_n(T) = T^n - T^{n-1} - y$$

Remarquons que ces polynômes sont tous irréductibles dans $\mathbb{Q}(y)[T]$ car unitaires et de degré 1 en y. Nous allons montrer que pour tout $n \geqslant 1$, $\mathrm{Gal}(F_n/\mathbb{Q}(y)) = S_n$. Pour cela, on se place, comme de bien entendu, dans un corps de fractions rationnelles $\mathbb{Q}(x)$ et on introduit l'extension $\mathbb{Q}(x)/\mathbb{Q}(y)$ où $y = x^n - x^{n-1}$; alors le polynôme minimal de x sur $\mathbb{Q}(y)$ est évidemment F_n. Examinons la ramification ; la forme de la dérivée, $F_n'(T) = T^{n-2}(nT - (n-1))$, montre qu'hormis la valuation à l'infini, seules w_0 et $w_{\frac{n-1}{n}}$ sont ramifiées sur $\mathbb{Q}(y)$; de plus,

$$e\left(w_0/\mathbb{Q}(y)\right) = n - 1 \qquad \text{et} \qquad e\left(w_{\frac{n-1}{n}}/\mathbb{Q}(y)\right) = 2$$

Remarquant de plus que w_0 et $w_{\frac{n-1}{n}}$ ne prolongent pas la même valuation sur $\mathbb{Q}(y)$, on déduit, du critère de Van der Waerden-Dedekind, et du fait qu'en caractéristique zéro, toutes les extensions sont modérément ramifiées, que le groupe de Galois de F_n sur $\mathbb{Q}(y)$ contient un $(n-1)$-cycle et une transposition. Comme S_n est le seul des ses sous-groupes transitifs à vérifier cela, on a bien le résultat.

Comme le suggère Serre dans [22], on peut déduire des polynômes précédents des réalisations du groupe alterné A_n sur $\mathbb{Q}(y)$. Commençons par remarquer qu'il est impossible de réaliser A_n, si n est pair, avec un polynôme du type $F(T) - y$ avec $F \in \mathbb{Q}(T)$ de degré n. En effet, si x désigne une racine de F, alors on sait que la valuation $w_{x,\infty}$ est totalement ramifiée sur $\mathbb{Q}(y)$; par suite, le groupe de Galois $\mathrm{Gal}(F/\mathbb{Q}(y))$ contient un n-cycle qui est une permutation impaire.

D'après la formule de Swan (c.f. [19], II-3.2 Théorème 50), le discriminant de F_n se met sous la forme :

$$\mathrm{dis}(F_n) = (-1)^{\frac{(n+2)(n-1)}{2}} n^n y^{n-2} \left(y + \frac{(n-1)^{(n-1)}}{n^n}\right)$$

• Par conséquent, si n est pair, alors

$$\mathrm{dis}(F_n) = c^2 \times (-1)^{\frac{n+2}{2}} \left(y + \frac{(n-1)^{(n-1)}}{n^n}\right) \qquad \text{avec :} \qquad c = n^{n/2} y^{(n-2)/2}$$

Forçons ce discriminant à être un carré ; posons pour cela :

$$z = (-1)^{\frac{n+2}{2}} y^2 - \frac{(n-1)^{n-1}}{n^n} \qquad \text{et} \qquad G_n(T) = T^n - T^{n-1} - z$$

Alors, nous avons tout fait pour qu'il en soit ainsi,

$$\mathrm{dis}(G_n) = c^2 y^2 \qquad \text{avec} \quad c \in \mathbb{Q}(z) \subset \mathbb{Q}(y)$$

Par conséquent, $\mathrm{dis}(G_n)$ est un carré dans $\mathbb{Q}(y)$. Le groupe de Galois $\mathrm{Gal}(G_n/\mathbb{Q}(y))$ est donc inclus dans A_n. Nous allons établir l'égalité.

L'élément z est encore une indéterminée sur $\mathbb{Q}$; prenons le corps des fractions rationnelles $\mathbb{Q}(z)$ comme corps de base momentanément. On sait, c'est le premier exemple traité, que $\mathrm{Gal}(G_n/\mathbb{Q}(z)) = S_n$. Cela étant, de manière classique, on considère x une racine de G_n et on s'intéresse à l'extension $\mathbb{Q}(x)/\mathbb{Q}(z)$. Notons L la clôture galoisienne de $\mathbb{Q}(x)$ sur $\mathbb{Q}(z)$. Pour conclure, vérifions que le schéma suivant est valide :

$$\begin{tikzcd}
L \arrow[dr, dash] \arrow[dd, dash, "A_n"'] & \\
& \mathbb{Q}(y)(x) \arrow[dl, dash, "n"] \arrow[d, dash] \\
\mathbb{Q}(y) \arrow[d, dash, "2"'] & \mathbb{Q}(x) \arrow[dl, dash, "n"] \\
\mathbb{Q}(z) &
\end{tikzcd}$$

ce qui revient à montrer que :

1. l'indéterminée y appartient au corps L et que, de plus, $\mathbb{Q}(y) = L^{A_n}$;
2. l'élément x, qui est degré n sur $\mathbb{Q}(z)$, est encore de degré n sur $\mathbb{Q}(y)$.

Dès lors, on aura bien montré que $\mathrm{Gal}(G_n/\mathbb{Q}(y)) = A_n$.

Commençons par s'assurer que $y \in L$. Par construction, on sait que $\mathrm{dis}(G_n) = c^2 y^2$ avec $c \in \mathbb{Q}(z)$. Mais si on désigne par $\sigma_1, \ldots, \sigma_n$ les n $\mathbb{Q}(z)$-homomorphismes de $\mathrm{Hom}_{\mathbb{Q}(z)}(\mathbb{Q}(x), L)$, alors $\mathrm{dis}(G_n)$ vérifie aussi :

$$\mathrm{dis}(G_n) = \prod_{i<j} (\sigma_i(x) - \sigma_j(x))^2 \qquad \sigma_i(x) \in L$$

c'est donc le carré d'un élément de L. Par suite, on a bien $y \in L$. Ainsi, on peut considérer la chaîne d'extensions $L/\mathbb{Q}(y)/\mathbb{Q}(z)$. Mais z étant un polynôme en y de degré 2 on sait que $[\mathbb{Q}(y) : \mathbb{Q}(z)] = 2$; comme de plus, A_n est l'unique sous groupe d'indice 2 dans S_n, la correspondance galoisienne donne nécessairement :

$$L^{A_n} = \mathbb{Q}(y)$$

Pour finir, il faut encore vérifier que x reste de degré n sur $\mathbb{Q}(y)$; il suffit, pour cela de s'assurer que le polynôme $G_n \in \mathbb{Q}(y)[T]$ est irréductible sur $\mathbb{Q}(y)$. Mais ce dernier, vu comme un polynôme de $\mathbb{Q}(T)[y]$ est de la forme $\pm y^2 - \mathrm{cste}$. Pour qu'un tel polynôme soit irréductible, il suffit que la constante ne soit pas un carré (ou l'opposé d'un carré selon le signe du coefficient dominant). Sauf dans le cas $n = 2$, on vérifie aisément que c'est le cas ; en effet, le pgcd de la constante et de sa dérivée (en T) est de degré 1 ($\mathrm{pgcd}(\mathrm{cste}, \mathrm{cste}') = T - (n-1)/n$), si bien que pour $n \geqslant 4$, G_n est nécessairement irréductible sur $\mathbb{Q}(y)$. En revanche, le polynôme G_2 est lui réductible : $G_2 = y^2 - (T^2 - T + 1/4) = (y - T + 1/2)(y + T - 1/2)$, mais dans ce cas nous sommes en train de chercher un polynôme qui réalise $A_2 = \{\mathrm{id}\}$ sur $\mathbb{Q}(y)$, ce qui ne présente qu'un maigre intérêt non ?

• Si n est impair, alors :

$$\mathrm{dis}(F_n) = d^2 (-1)^{\frac{n-1}{2}} \left(n + \left(\frac{n-1}{n} \right)^{n-1} \frac{1}{y} \right) \qquad \text{avec :} \qquad d = n^{(n-1)/2} y^{(n-1)/2}$$

Ainsi, en posant cette fois :

$$u = \left(\frac{n-1}{n} \right)^{n-1} \frac{1}{(-1)^{\frac{n-1}{2}} y^2 - n} \qquad \text{et} \qquad G_n(T) = T^n - T^{n-1} - u$$

on obtient, pour chaque entier n impair, un polynôme G_n de degré n et de groupe de Galois A_n sur $\mathbb{Q}(y)$.

En résumé, nous venons d'établir que :

Proposition 27 *Soit y une indéterminée sur $\mathbb{Q}$ et $n \geqslant 1$ un entier ; on pose $\alpha_n = \left(\frac{n-1}{n}\right)^{n-1}$ et $\varepsilon_n = (-1)^{\frac{(n-1)(n+2)}{2}}$. Alors les polynômes F_n et $G_n \in \mathbb{Q}(y)[T]$ définis par :*

$$F_n(T) = T^n - T^{n-1} - y \qquad \text{et} \qquad G_n(T) = \begin{cases} T^n - T^{n-1} - (\varepsilon_n y^2 - \dfrac{\alpha_n}{n}) & \text{si } n \text{ est pair} \\ T^n - T^{n-1} - \dfrac{\alpha_n}{\varepsilon_n y^2 - n} & \text{si } n \text{ est impair} \end{cases}$$

ont S_n et A_n pour groupes de Galois respectifs sur $\mathbb{Q}(y)$.

II.7.3 D'autre exemples en caractéristique non nulle

Pour se convaincre, si nécessaire une nouvelle fois, de l'utilité d'examiner les groupes de décomposition et d'inertie associés à une valuation ramifiée, un "bon terrain" est celui des corps munis de valuations discrètes à corps résiduels algébriquement clos comme par exemple, les corps de fractions rationnelles sur un corps algébriquement clos. En effet, sur de tels corps, les valuations non ramifiées ne sont d'aucune utilité puisque les groupes de décomposition et d'inertie sont triviaux. En revanche, les groupes d'inertie (qui sont égaux aux groupes de décomposition) portent, eux, de l'information. Traitons une nouvelle fois un exemple.

Soit k un corps algébriquement clos de caractéristique $p \neq 0$ et $k(x)$ une extension pure de degré de transcendance 1. On s'intéresse aux polynômes (dûs à Abhyankar, c.f.[1]) de la forme :

$$F_{q,r}(Y) = Y^n - xY^r + 1 \qquad \text{avec} \quad \begin{cases} q \text{ une puissance positive de } p, \\ n = q + r, \\ r \geqslant 1 \quad \text{et} \quad r \not\equiv 0 \mod p \end{cases}$$

Comme nous allons pouvoir le constater, cette classe de polynômes réalise un certain nombre de groupes de Galois sur le corps $k(x)$.

Tout d'abord, les polynômes $F_{q,r}$ sont irréductibles dans $k(x)[Y]$ car primitifs et de degré 1 en x. Ensuite, par hypothèse, n et r sont premiers entre eux ; ainsi la formule de Swan (c.f. [19], II-3.2 Théorème 50) nous montre que :

$$\operatorname{dis}(F_{q,r}) = (-1)^{n(n-1)/2}\left(n^n - (-1)^n (n-r)^{n-r} r^r x^n\right) = (-1)^{n(n-1)/2} n^n \in k \qquad \text{car } n - r \equiv 0 \mod p$$

En particulier, comme $n \not\equiv 0 \pmod p$, les polynômes $F_{q,r}$ sont séparables. De plus, le corps k étant supposé algébriquement clos, $\operatorname{dis}(F_{q,r})$ est donc un carré dans $k \subset k(x)$; si la caractéristique de k est **distincte de 2**, i.e. $p \neq 2$, alors $\operatorname{Gal}(F_{q,r}/k(x)) \subset A_n$.

> **Remarque** – Dans $\mathbb{F}_{q^2}$, $\operatorname{dis}(F_{n,r})$ est déjà un carré. Le caractère algébriquement clos du corps de base k n'est pas encore fondamental.

Nous traiterons séparément les cas $r = 1$ et $q = p$, $r \geqslant 3$. Cependant, l'étude de la ramification sera utile à chaque fois. Notons y une racine de $F_{q,r}$ alors nous considérerons bien sûr l'extension $k(x,y)/k(x)$. En fait $x \in k(y)$ car :

$$x = \frac{y^{q+r} + 1}{y^r},$$

et l'extension $k(y)/k(x)$ est de degré $n = q + r$, la hauteur de la fraction rationnelle en y donnée ci-avant. Le numérateur de la dérivée de cette fraction rationnelle étant constant, on vérifie facilement que $v_{x,\infty}$ est la seule valuation sur $k(x)$ (triviale sur k) qui se ramifie dans $k(y)$; plus précisément, $v_{x,\infty}$ se factorise sous la forme :

$$v_{x,\infty} = v_{y,\infty}^q v_{y,0}^r$$

Cela étant, nous pouvons désormais traiter les cas particuliers :

Supposons que $n = p + r$ **avec** $r \geqslant 3$ **et** $r \not\equiv 0 \pmod p$ **:**

Montrons que si tel est le cas, alors :

$$\operatorname{Gal}(F_{p,r}/k(x)) = \begin{cases} S_n & \text{si } p = 2 \\ A_n & \text{sinon} \end{cases}$$

Notons y une racine de $F_{p,r}$ alors on se ramène bien sûr à l'étude de la situation suivante :

$$\begin{tikzcd} L = k(y)^{\mathrm{gal}} \arrow[dd, dash, "\Gamma"'] \arrow[dr, dash] & \\ & E = k(y) \\ K = k(x) \arrow[ur, dash, "n"'] & \end{tikzcd} \qquad \underline{k(y)} = \operatorname{Hom}_{k(x)}(k(y), k(y)^{\mathrm{gal}}) = \underline{E} = \operatorname{Hom}_K(E, L)$$

Nous avons montré précédemment que :

$$v_{x,\infty} = v_{y,\infty}^p v_{y,0}^r$$

Notons pour alléger $v = v_{x,\infty}$, $v_1 = v_{y,\infty}$, $v_2 = v_{y,0}$, w un prolongement de v à L et K_v, E_1, E_2, L_w les complétés respectifs de K pour v, de E pour v_1 et v_2 et enfin de L pour w. Alors compte tenu de ce qui précède, on a le diagramme :

$$\begin{tikzcd}
 & D(E_1^{\mathrm{gal}}/K_v) & \\
D(L_w/K_v) \arrow[ur, two heads, "r_1"] \arrow[dr, two heads, "r_2"'] \arrow[rr, hook] & & D(E_1^{\mathrm{gal}}/K_v) \times D(E_2^{\mathrm{gal}}/K_v) \arrow[ul, "\pi_1"'] \arrow[dl, "\pi_2"] \\
 & D(E_2^{\mathrm{gal}}/K_v) &
\end{tikzcd}$$

(où r_1, r_2 sont les morphismes de restriction et π_1, π_2 les projections). Cela nous permet de nous concentrer sur les deux situations locales : E_1/K_v et E_2/K_v. La première extension (de degré p) est totalement et fortement ramifiée alors que la seconde (de degré r) est totalement et modérément ramifiée. Dès lors, concernant les groupes de décomposition "locaux", on a :

• le groupe $D(E_1^{\mathrm{gal}}/K_v)$ est un sous-groupe de S_p qui agit transitivement sur un ensemble à p éléments (à savoir $\underline{E_1} = \mathrm{Hom}_{K_v}(E_1, L_w)$) ; par suite il contient un p-cycle. Ce dernier admet un antécédent dans $D(L_w/K_v)$ par r_1 que l'on note σ.

• l'extension E_2/K_v étant modérément et totalement ramifiée, c'est une extension galoisienne de surcroît cyclique. Par conséquent, $E_2 = E_2^{\mathrm{gal}}$ et $D(E_2^{\mathrm{gal}}/K_v)$ est cyclique d'ordre r. Notons τ un antécédent d'un des générateurs de $D(E_2^{\mathrm{gal}}/K_v)$ par r_2.

De ces deux points, on déduit que σ^r est p-cycle (car r est premier avec p) dont le support est le sous-ensemble $\underline{E_1}$. Quant à l'élément τ, il vérifie $\tau(\underline{E_1}) = \underline{E_1}$ et c'est un r-cycle sur $\underline{E} \setminus \underline{E_1} = \underline{E_2}$. Ainsi, Γ est nécessairement primitif comme le confirme le lemme suivant :

Lemme 7 *Soit G un groupe fini agissant transitivement sur un ensemble fini X. On suppose que G contient un s-cycle σ de support S et un élément τ tel que $\tau(S) = S$ et $\tau_{|X \setminus S}$ soit un r-cycle (où $r = \#(X \setminus S)$). Si s et r sont premiers entre eux alors G est primitif.*

Preuve — Ecrivons :

$$X = S \vee R \qquad \text{avec} \quad \#S = s \quad \text{et} \quad \#R = r$$

et considérons $B \subset X$ un bloc d'imprimitivité, c'est à dire un sous-ensemble de X tel que $gB = B$ ou $gB \cap B = \varnothing$ pour tout $g \in G$. Il faut vérifier que B est soit réduit à un singleton soit l'ensemble X tout entier. • En premier lieu, on suppose que B rencontre à la fois S et R et on montre qu'alors $B = X$. Soit $t_0 \in B \cap R$ alors $\sigma(t_0) = t_0 \in B \cap \sigma(B)$ et donc $\sigma(B) = B$; ainsi, $\sigma(B \cap S) = B \cap S$ et $B \cap S$ est une partie non vide de S stable par le groupe $\langle \sigma_{|S} \rangle$ qui agit transitivement sur S. Nécessairement $B \cap S = S$ ou encore $S \subset B$.

Maintenant $\varnothing \neq S = \tau(S) \cap S \subset B \cap \tau(B)$, donc $\tau(B) = B$. Comme précédemment, on en déduit que $R \subset B$, i.e. $X = B$

• Soit B un bloc d'imprimitivité différent de X. Alors la famille des gB pour $g \in G$ forme une partition de X en sous-ensembles tous de même cardinal à savoir $\#B$. D'après ce qui précède, ou bien $gB \subset S$ ou bien $gB \subset R$; par conséquent $\#B$ divise à la fois s et r. Ces deux entiers étant par hypothèse premiers entre eux, on a nécessairement $\#B = 1$, d'où le résultat. □

Pour conclure, nous allons utiliser un autre résultat de théorie des groupes à savoir (c.f. [11], Chap XII, §3, Théorème 3.7) :

Théorème 8 (Jordan) *Si un groupe G primitif de degré $n = p + r$ contient un p-cycle, où p est premier et $r \geqslant 3$, alors $G = A_n$ ou S_n.*

Compte tenu de ce qui précède,

- si $p \neq 2$, on a donc $\Gamma = A_n$;
- si $p = 2$, Γ contient une transposition et est primitif donc $\Gamma = S_n$.

Supposons désormais $r = 1$

On considère cette fois le polynôme $F_{q,1}$ (où q est, je le rappelle une puissance de p) à coefficients dans $k(x)$ où k est un corps algébriquement clos de caractéristique p :

$$F_{q,1}(Y) = Y^{q+1} - xY + 1$$

Je m'inspire ici de la belle lettre de J-P.Serre qui figure en appendice à l'article d'Abhyankar (c.f.[1]). Il s'agit de montrer que $\mathrm{Gal}(F_{q,1}/k(x)) = PSL_2(\mathbb{F}_q)$. Contrairement à la méthode employée pour $r \geqslant 3$, où nous nous "attaquions de front" à l'équation[12] $F_{q,r}$, nous allons partir ici d'une $PSL_2(\mathbb{F}_q)$-extension de $k(z)$ (où z est une indéterminée sur k) pour en construire une autre pouvant être réalisée comme la clôture galoisienne du corps engendré par une racine de $F_{q,1}$. Nous serons guidés dans cette quête de la "bonne extension" par le **type de la ramification** de cette dernière :

$$\begin{tikzcd}
k(x,y)^{\mathrm{gal}} \arrow[dd, dash, "PSL_2(\mathbb{F}_q)"'] \arrow[dr, dash] & \\
& k(x)(y) \\
k(x) \arrow[ur, dash] &
\end{tikzcd} \qquad \text{avec} \quad F_{q,1}(y) = 0$$

En effet, comme le montre l'étude de la ramification préliminaire à cet exemple, **seule** la valuation $v_{x,\infty}$ est ramifiée dans $k(x,y)^{\mathrm{gal}}$; cet piste sera fondamentale dans la suite...

On part d'une extension galoisienne $k(t)/k(z)$ de groupe de Galois égal $PGL_2(\mathbb{F}_q)$; pour cela, on introduit :

$$z = \frac{(t^{q^2} - t)^{q+1}}{(t^q - t)^{q^2+1}}$$

(c.f. exercice 36 du chapitre VI de [14]). On vérifie facilement que cette fraction est invariante par $PGL_2(\mathbb{F}_q)$;

Remarques

1. Rappelons qu'il y a un morphisme (surjectif) de groupes entre $GL_2(k)$ et $\mathrm{Aut}_k(k(t))$ qui est donné par (la surjectivité est une conséquence de Luröth) :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \left\{ t \mapsto \frac{at+c}{bt+d} \right\} \qquad \text{(Attention à la \textbf{transposée} !)}$$

(on ne fait pas correspondre l'automorphisme $t \mapsto \frac{at+b}{ct+d}$ pour que ce morphisme en soit un !). Le noyau est formé des homothéties. Par passage au quotient on obtient donc un isomorphime de groupes entre $PGL_2(k)$ et $\mathrm{Aut}_k(k(t))$.

D'autre part, $PGL_2(k)$ opère (transitivement) sur $\mathbb{P}_1(k)$. L'action est, cette fois, donnée par :

$$\begin{array}{ccc} PGL_2(k) & \longrightarrow & \mathrm{Perm}(\mathbb{P}_1(k)) \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longmapsto & \left(\lambda \mapsto \frac{a\lambda+b}{c\lambda+d}\right) \end{array}$$

2. Pour vérifier la stabilité de z sous l'action de $PGL_2(\mathbb{F}_q)$, une manière simple de conduire les calculs est de vérifier que :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.(t^q - t) = (ad-bc)\frac{t^q - t}{(bt+d)^{q+1}} \qquad \text{et} \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix}.(t^{q^2} - t) = (ad-bc)\frac{t^{q^2} - t}{(bt+d)^{q^2+1}}$$

Nous utiliserons ces formules dans la suite pour nous convaincre de la stabilité d'une autre fraction rationnelle sous l'action d'un autre groupe.

De plus, elle est de bonne hauteur, à savoir $\#PGL_2(\mathbb{F}_q) = q^3 - q$, car :

$$z = \frac{[(t^q - t)^q + (t^q - t)]^{q+1}}{(t^q - t)^{q+1}(t^q - t)^{q^2 - q}} = \frac{\left[(t^q - t)^{q-1} + 1\right]^{q+1}}{(t^q - t)^{q^2 - q}}$$

qui est clairement la forme irréductible de z.

Ainsi, on obtient un sous-corps $k(z)$ de $k(t)$ tel que l'extension $k(t)/k(z)$ soit galoisienne de goupe de Galois égal à $PGL_2(\mathbb{F}_q)$. Si $p = 2$, comme $PGL_2(\mathbb{F}_q) = PSL_2(\mathbb{F}_q)$, on a en fait une $PSL_2(\mathbb{F}_q)$-extension. Si p est impair, alors d'après la définition de z, $z^{1/2} \in k(t)$. Rappelons maintenant qu'une matrice de $GL_2(\mathbb{F}_q)$ a une image dans $PSL_2(\mathbb{F}_q)$ si et seulement si le déterminant de cette dernière est un carré (non nul) dans $\mathbb{F}_q$. Tenant compte de cette remarque, et des formules données plus haut, on se convainc facilement du fait que $z^{1/2}$ est $PSL_2(\mathbb{F}_q)$-stable. Comme cette fraction rationnelle est de bonne hauteur, l'extension $k(t)/k(z^{1/2})$ est galoisienne de groupe de Galois égal à $PSL_2(\mathbb{F}_q)$.

Jusque là, comme le dit J-P.Serre, la méthode employée est très classique. Le problème est qu'elle ne fournira jamais l'équation cherchée, $F_{q,1}$. En effet, comme nous l'a montré l'étude de la ramification au début de cet exemple, si $k(t)$ est le corps de décomposition de $F_{q,1}$ sur $k(x)$, alors **seule** la valuation $v_{x,\infty}$ est ramifiée dans $k(t)$. Or ici, l'examen de la ramification dans l'extension $k(t)/k(z)$ montre que (on s'aide de la proposition 24 pour établir ce qui suit) :

[12] En revanche, Abhyankar dans son article ne change pas de stratégie pour $r = 1$, ni pour $r = 2$ d'ailleurs. Son point de départ reste toujours l'équation $F_{q,r}$, dont il détermine le groupe de Galois en le cernant de plus en plus. Il utilise pour cela des résultats de classification des groupes.

• En tout point $\lambda \in \mathbb{F}_q \cup \{\infty\}$, la valuation $v_{t,\lambda}$ est ramifiée sur $k(z)$, d'incide de ramification égal à $(q^2 - q)$. Plus précisément :

$$(v_{t,\lambda})_{|k(z)} = (q^2 - q) \times v_{z,\infty}$$

• En tout point $\lambda \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, la valuation $v_{t,\lambda}$ est ramifiée sur $k(z)$, d'indice de ramification $(q + 1)$ et vérifie :

$$(v_{t,\lambda})_{|k(z)} = (q + 1) \times v_{z,0}$$

• En dehors des points précédents, il n'y a pas ramification.

Ainsi, "renversant la vapeur", nous venons de montrer que seules les valuations $v_{z,0}$ et $v_{z,\infty}$ sont ramifiées dans $k(t)$ la première l'étant **modérément** la seconde **fortement**. Pour espérer obtenir l'équation $F_{q,1}$, il y a donc une valuation ramifiée de trop. Qu'à cela ne tienne, nous allons nous **"débarrasser"** de la ramification au dessus de $v_{z,0}$. C'est dans ce but là que J-P.Serre introduit l'élément x tel que :

$$z = x^{q+1}$$

On effectue alors une translation (au sens de Bourbaki, [5], Chap V, §10, n°8) en étendant le corps de base à $k(x)$ (qui est une extension galoisienne (cyclique) de $k(z)$). Il convient tout de même de vérifier que le groupe de Galois n'est pas modifié (au pire il a diminué), et qu'une **seule** valuation de $k(x)$ est ramifiée dans $k(x, t)$. Rappelons pour cela un classique de la théorie de Galois (c.f.[5], Chap V, §10, n°8) :

Proposition 28 *Un corps Ω algébriquement clos contenant les corps à suivre étant fixé, on considère L/K une extension (finie) galoisienne, K' un sur-corps de K et on note L' le compositum de L et K'. Si $L \cap K' = K$ alors l'extension L'/K', que l'on sait être galoisienne vérifie :*

$$\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(L'/K')$$

En conséquence, on a l'égalité dimensionnelle $[L' : K'] = [L : K]$ et on en déduit que K' et L sont linéairement disjoints sur K.

Si p est impair, pour utiliser la proposition précédente à notre cadre, il faut montrer que $k(t) \cap k(x) = k(z^{1/2})$, ce qui revient à montrer l'égalité dimensionnelle :

$$[k(x, t) : k(t)] = [k(x) : k(z^{1/2})]$$

$$\begin{tikzcd}
 & k(x,t) \arrow[dl, dash] \arrow[dr, dash, "PSL_2(\mathbb{F}_q)\ ?"] & \\
k(t) \arrow[dr, dash, "PSL_2(\mathbb{F}_q)"] \arrow[ddr, dash, "PGL_2(\mathbb{F}_q)"'] & & k(x) \arrow[dl, dash] \arrow[ddl, dash, "C_{q+1}"] \\
 & k(z^{1/2}) \arrow[d, dash, "2"'] & \\
 & k(z) &
\end{tikzcd}$$

On est donc ramené (par exemple) à vérifier que x, qui est algébrique de degré $(q+1)/2$ sur $k(z^{1/2})$, reste de degré $(q+1)/2$ sur $k(t)$. Mais $x^{q+1} = z$ donc $x^{\frac{q+1}{2}} = z^{1/2}$ ou encore en revenant à t :

$$x^{\frac{q+1}{2}} - \frac{\left[(t^q - t)^{q-1} + 1\right]^{\frac{q+1}{2}}}{(t^q - t)^{\frac{q^2-q}{2}}} = 0$$

Par suite x est de degré inférieur à $(q + 1)/2$ sur $k(t)$.

Pour établir l'égalité, il faut vérifier que le polynôme $P \in k(t)[X]$ défini par :

$$P(X) = X^{\frac{q+1}{2}} - \frac{f(t)}{g(t)} \qquad \text{avec :} \quad \begin{cases} f, g \in k[t] \text{ premiers entre eux} \\ \deg(f) = \frac{q(q-1)(q+1)}{2} \\ \deg(g) = \frac{q^2(q-1)}{2} \end{cases}$$

est irréductible. Ce polynôme P est de la forme $X^n - a$; un résultat classique (c.f.[14], Chap VI, §9, Théorème 9.1. Notons que dans notre cadre la démonstration en est considérablement simplifiée car le corps k contient les racines n-èmes de l'unité), affirme que P est irréductible dans $k(t)[X]$ si et seulement si :

1. pour tout premier l divisant $\deg(P) = \frac{q+1}{2}$, $f/g \notin k(t)^l$,

2. et si 4 divise $\frac{q+1}{2}$ alors $f/g \notin -4k(t)^4$, qui est impliqué par $-4f/g \notin k(t)^4$.

Ce critère s'applique facilement ici ; en effet, pour qu'une fraction rationnelle R soit une puissance l-ème dans $k(t)$, il faut que les degrés du numérateur et du dénominateur de sa décomposition irréductible soient multiples de l. Les entiers $\frac{q+1}{2}$ et $\frac{q^2(q-1)}{2}$ étant premiers entre eux (car $\frac{q+1}{2}$ est premier à la fois avec q et et avec $\frac{q-1}{2}$), nécessairement $\deg(g)$ n'est pas un multiple de l (si l divise $\frac{q+1}{2}$). Par suite, la fraction rationnelle, f/g n'est pas une puissance l-ème. De même $-4f/g$ n'est pas une puissance quatrième. Les hypothèses du critère sont donc vérifiées ; le polynôme P est irréductible sur $k(t)$ et x est bien de degré $(q+1)/2$ sur $k(t)$.

Si $p = 2$, on procède de même en utilisant le fait que $(q+1)$ et $q^2(q-1)$ sont premiers entre eux cette fois.

Dans tous les cas, l'extension $k(x)(t)/k(x)$ est donc galoisienne de groupe de Galois égal à $PSL_2(\mathbb{F}_q)$. Et du point de vue de la ramification, que pouvons-nous dire ? Si cette manipulation représente un réel gain, de notre point de vue, alors **seule** une valuation de $k(x)$ doit être ramifiée dans $k(x,t)$. C'est en effet le cas. Notons que seules les valuations de $k(z)$, $v_{z,0}$ et $v_{z,\infty}$, sont ramifiées dans $k(x)$, toutes deux d'indice de ramification égal à $(q+1)$ (pour s'en convaicre, s'aider de la proposition 24) ; mieux :

$$v_{x,0} = (q+1) \times v_{z,0} \qquad \text{et} \qquad v_{x,\infty} = (q+1) \times v_{z,\infty}$$

Ainsi, seuls les prolongements de $v_{z,0}$ et $v_{z,\infty}$ à $k(x)$ sont susceptibles d'être ramifiés dans $k(t,x)$ (le compositum de deux extensions non ramifiées est non ramifié). Considérons désormais w un prolongement de $v_{x,0}$ à $k(x,t)$. Alors w se restreint nécessairement à $k(z)$ en $v_{z,0}$. Par suite, la restriction de w au corps $k(t)$ est l'une des valuations $v_{t,\lambda}$ pour $\lambda \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$; cette dernière est, on le sait, modérement ramifiée sur $k(z)$, d'indice de ramification égal à $(q+1)$. Grâce au lemme d'Abhyankar dont l'énoncé figure déjà dans une remarque d'une section précédente (c.f. lemme 6), on en déduit, en complétant que $v_{x,0}$ n'est pas ramifié dans $k(x,t)$ car :

$$e(v_{t,\lambda}/k(z)) = q+1 = e(v_{x,0}/k(z)) \not\equiv 0 \mod p\ ;$$

Ainsi, **seul** $v_{x,\infty}$, l'unique prolongement de $v_{z,\infty}$ à $k(x)$ est ramifié dans $k(x,t)$. Cette fois on dispose bien d'une $PSL_2(\mathbb{F}_q)$-extension ramifiée en un seul point (i.e. l'infini). Il ne reste plus qu'à vérifier qu'elle permet de trouver l'équation cherchée. Autrement dit, on cherche maintenant, un élément de $k(t,x)$ dont le polynôme minimal sur $k(x)$ soit égal à $F_{q,1}$ et de corps de décomposition égal à $k(t,x)$.

Pour cela, on redescend une nouvelle fois au niveau de $k(z)$. Introduisons H le sous-groupe de $PGL_2(\mathbb{F}_q)$ formé des automorphismes :

$$H = \{t \mapsto at + b \ a \in \mathbb{F}_q^*,\ b \in \mathbb{F}_q\}$$

Remarque – Ici, tout se passe dans $\mathrm{Aut}_k(k(t))$. Compte tenu de l'isomorphisme entre $PGL_2(\mathbb{F}_q)$ et $\mathrm{Aut}_k(k(t))$, H est isomorphe au sous-groupe de $PGL_2(\mathbb{F}_q)$ formé des matrices :

$$\left\{ \begin{pmatrix} a & 0 \\ c & 1 \end{pmatrix},\ a \in \mathbb{F}_q^*,\ c \in \mathbb{F}_q \right\}$$

Ce sous-groupe est le stabilisateur de 0 pour l'action de $PGL_2(\mathbb{F}_q)$ sur $\mathbb{P}_1(\mathbb{F}_q)$. A noter qu'il existe un automorphisme de $PGL_2(\mathbb{F}_q)$ qui envoie ce sous-groupe sur le classique $AGL_1(\mathbb{F}_q)$, stabilisateur de l'infini :

$$AGL_1(\mathbb{F}_q) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix},\ a \in \mathbb{F}_q^*,\ b \in \mathbb{F}_q \right\}$$

Le corps intermédiaire, $k(t)^H$; ce dernier est engendré par $y = (t^q - t)^{q-1}$ car ce polynôme est invariant par H et de bonne hauteur, à savoir $\#H = q^2 - q$. Un petit schéma pour résumer :

$$\begin{tikzcd}
k(t) \arrow[dd, dash, "PGL_2(\mathbb{F}_q)"'] \arrow[dr, dash, "q^2-q"] & \\
& k(y) = k(t)^H \\
k(z) \arrow[ur, dash, "q+1"'] &
\end{tikzcd}$$

Vérifions que $k(y)^{\text{gal}} = k(t)$; c'est vrai si (et seulement si) l'intersection des conjugués de H dans $PGL_2(\mathbb{F}_q)$ est réduite à l'identité. Faisons opérer, de manière classique $PGL_2(\mathbb{F}_q)$ sur $\mathbb{P}_1(\mathbb{F}_q)$; cette opération est fidèle et transitive et H n'est rien d'autre que le stabilisateur de 0 (c.f. remarque précédente) pour cette action. Nécessairement l'intersection des conjugués de H est donc réduite à l'identité, ce que l'on voulait. Maintenant, dans le cas où p est impair, peut-on "remonter" à $k(z^{1/2})$; autrement dit a-t'on "2" à la place de “?” dans le schéma suivant ?

$$\begin{tikzcd}[arrows=dash]
k(t) \arrow[dd, "PSL_2(\mathbb{F}_q)"'] \arrow[dr] & \\
 & k(z^{1/2})(y) \arrow[d, "?"] \arrow[dl] \\
k(z^{1/2}) \arrow[d, "2"'] & k(y) \arrow[dl, "q+1"] \\
k(z) &
\end{tikzcd}$$

Cela revient à montrer que $z^{1/2} \notin k(y)$. Mais dans le cas contraire, revenant aux définitions respectives de $k(z^{1/2})$ et $k(y)$, on déduit :

$$k(t)^{PSL_2(\mathbb{F}_q)} \subset k(t)^H \quad \text{donc} \quad H \subset PSL_2(\mathbb{F}_q)$$

ce qui est faux (sauf si $q = 2$).

Et maintenant, peut-on remonter à $k(x)$? La réponse est positive et découle d'un corollaire de la proposition 28 :

Corollaire 7 *Sous les hypothèses de la proposition 28, il y a une correspondance bi-univoque entre les sous-corps de L/K et ceux de L'/K' ; cette correspondance est donnée par : à E un sous-corps de L on associe le sous-corps $K'E$, à E' un sous-corps de L' on associe le sous-corps $E' \cap L$.*

Ainsi, si E un sous-corps de L vérifiant $E^{\text{gal}} = L$, alors le sous corps $K'E$ qui lui correspond vérifie $(K'E)^{\text{gal}} = L'$. Par conséquent, l'élément y vérifie encore :

$$k(x)(y)^{\text{gal}} = k(x, t)$$

Pour finir, et là je suis tout de même étonné, rappelons que :

$$z = \frac{(y+1)^{q+1}}{y^q} \quad \Rightarrow \quad (y+1)^{q+1} - x^{q+1}y^q = 0 \quad \Rightarrow \quad \left(\frac{y+1}{xy}\right)^{q+1} - x\left(\frac{y+1}{xy}\right) + 1 = 0$$

Par suite, posant $y' = (y+1)/xy$, alors $k(x, y) = k(x, y')$ (car $y = \frac{1}{xy'-1}$) et y' est une racine du polynôme $F_{q,1}$; y' est l'élément cherché.

En bref, nous venons d'établir le résultat :

Proposition 29 *Soit k un corps algébriquement clos de caractéristique p non nulle. Pour q une puissance de p et $r \geqslant 1$ un entier premier avec p, on considère le polynômes $F_{q,r} \in k(x)[Y]$ (où x est une indéterminée sur k) défini par :*

$$F_{q,r}(Y) = Y^{q+r} - xY^r + 1$$

alors on a :

1. *si $q = p = 2$ et $r \geqslant 3$ alors $\text{Gal}(F_{q,r}/k(x)) = S_n$;*
2. *si $q = p \neq 2$ et $r \geqslant 3$ alors $\text{Gal}(F_{q,r}/k(x)) = A_n$;*
3. *si $r = 1$ alors $\text{Gal}(F_{q,r}/k(x)) = PSL_2(\mathbb{F}_q)$.*

Pour les cas ne figurant pas dans la proposition précédente, en particulier le cas $r = 2$, je renvoie le lecteur à [1], §21 : “The bar polynomial”.

III Racines de polynômes à coefficients dans un corps complet

Dans toute cette section, K est un corps **complet** pour une valeur absolue $|\ |$ **ultra-métrique**. On note A l'anneau de valuation pour K associé à $|\ |$ (on dit aussi, par abus de langage, que A est l'anneau des entiers de K) et $\mathfrak{m}$ son idéal maximal. Je rappelle que :

$$A = \{x \in K,\ |x| \leqslant 1\} \quad \text{et} \quad \mathfrak{m} = \{x \in K,\ |x| < 1\}$$

Comme exemple de corps vérifiant les hypothèses précédentes, on a bien sûr $K = \mathbb{Q}_p$ muni de la valeur absolue p-adique $|\ |_p$. Alors $A = \mathbb{Z}_p$ et $\mathfrak{m} = p\mathbb{Z}_p$. Toutes les extensions de degré fini de $\mathbb{Q}_p$ munies de l'unique prolongement de $|\ |_p$ fournissent aussi un grand nombre d'exemples intéressants.

Avant toute chose, il est un argument utilisé constamment dans cette section ; je préfère donc le mettre en avant. Il s'agit d'une des nombreuses conséquences de "l'ultra-métricité" de la valeur absolue :

$$\forall x, y \in K, \qquad |x - y| < |x| \quad \Longrightarrow \quad |x| = |y|. \tag{P1}$$

De manière équivalente, on peut dire :

$$\forall x, y \in K, \qquad |y| < |x| \quad \Longrightarrow \quad |x + y| = |x|. \tag{P1'}$$

A de multiples reprises, nous utiliserons aussi le fait que :

$$\forall P \in A[X],\ \forall x, y \in A, \qquad |P(x) - P(y)| \leqslant |x - y|\ ; \tag{P2}$$

en effet, il suffit d'écrire $P(x) - P(y) = (x - y)Q(x, y)$ avec $Q \in A[X, Y]$ et remarquer que x et y étant entiers, $|Q(x, y)| \leqslant 1$.

Nous pouvons d'ores et déjà illustrer la portée des ces deux résultats élémentaires. Considérons par exemple deux éléments x et y de A et un polynôme $P \in A[X]$ qui vérifient :

$$|x - y| < |P(x)|.$$

A priori, cette propriété n'est pas symétrique en x et y. Pourtant, en vertu de P2,

$$|P(x) - P(y)| \leqslant |x - y| < |P(x)|\ ;$$

ainsi d'après P1, $|P(x)| = |P(y)|$. Les éléments x et y jouent donc un rôle symétrique. En résumé, nous avons montré que :

$$\forall P \in A[X],\ \forall x, y \in A, \qquad |x - y| < |P(x)| \quad \Longrightarrow \quad |P(x)| = |P(y)|. \tag{P3}$$

III.1 La méthode de Newton

Le résultat fondamental de cette section est une reformulation de la méthode de Newton, grand classique d'analyse, dans le cadre des corps complets pour une valeur absolue ultra-métrique.

En guise d'introduction, je propose de résoudre l'exercice (élémentaire et classique) suivant : soit $a \in \mathbb{Z}$ un entier **impair** ; à quelle condition a est-il un carré modulo 2^k et plus particulièrement, connaissant une racine carré de a modulo 2^k, comment en calculer une modulo 2^{k+1} ? On part donc de $x \in \mathbb{Z}$ tel que $x^2 \equiv a \pmod{2^k}$ et on cherche à construire $x' \in \mathbb{Z}$ tel que ${x'}^2 \equiv a \pmod{2^{k+1}}$. Le réflexe classique consiste à écrire $x' = x + \lambda 2^k$ puis à exploiter la congruence ${x'}^2 \equiv a \pmod{2^{k+1}}$ pour calculer λ. Pourtant, le lecteur peut s'en convaincre tout seul, cette méthode est vouée à l'échec. En fait, il ne faut pas chercher à ce que x' "couvre" x modulo 2^k mais modulo 2^{k-1} ; cette petite subtilité est la seule difficulté de cet exercice ; en effet, si on pose $x' = x + \lambda 2^{k-1}$ alors la stratégie avortée ci-avant donne dans ce cas :

$$(x + \lambda 2^{k-1})^2 \equiv a \mod 2^{k+1} \qquad \text{i.e.} \qquad x^2 + \lambda x 2^k + \lambda^2 2^{2(k-1)} \equiv a \mod 2^{k+1}$$

Ainsi, supposant de plus que $2(k-1) \geqslant k+1$, c'est à dire $k \geqslant 3$ et remarquant que a étant impair, x l'est, on obtient :

$$\lambda \equiv \frac{x^2 - a}{2^k} \mod 2$$

En bref, si un entier a **impair** est un carré modulo 8, alors c'est un carré modulo toutes les puissances de 2. Autrement dit, pour que le polynôme $F(X) = X^2 - a$ admette une racine modulo toutes les puissances de 2, il suffit qu'il admette une racine x modulo 8, c'est à dire un entier $x \in \mathbb{Z}$ impair tel que :

$$v_2(F(x)) > 2v_2(F'(x)) \qquad \text{ou encore} \qquad |F(x)|_2 < |F'(x)|_2^2$$

Le lecteur peut recommencer l'exercice à partir du polynôme $F(x) = X^4 - a$ (a est toujours un entier impair) ; nous allons, dès maintenant, considérer le cas général, à savoir celui d'un polynôme F de $A[X]$ et d'un élément x de A satisfaisant à :

$$|F(x)| < |F'(x)^2|. \tag{$*$}$$

En particulier, $F'(x) \neq 0$, on peut donc introduire l'itéré de Newton défini par :

$$y = x - \frac{F(x)}{F'(x)}.$$

Grâce à l'hypothèse $(*)$, il vient que $y \in A$. Nous allons en fait montrer que l'itéré de Newton vérifie encore l'hypothèse $(*)$ et en déduire un procédé itératif.

Introduisons, pour z tel que $F'(z) \neq 0$ la quantité : $\rho_z = \left|\frac{F(z)}{F'(z)^2}\right|$. Reprenant les hypothèses du début, on montre que :

Lemme 8 *Soit K un corps muni d'une valeur absolue ultra-métrique $|\ |$; on note A l'anneau de valuation pour K associé à $|\ |$ et on considère $F \in A[X]$. Soit $x \in A$ tel que :*

$$|F(x)| < |F'(x)^2|. \tag{$*$}$$

Alors l'itéré de Newton de x, y défini par $y = x - \frac{F(x)}{F'(x)}$ vérifie :

$$|F'(y)| = |F'(x)| \qquad et \qquad \rho_y \leqslant \rho_x^2.$$

Preuve — Grâce à l'hypothèse $(*)$, on peut majorer la quantité $|y - x|$:

$$|y - x| = \left|\frac{F(x)}{F'(x)}\right| < |F'(x)| \ ;$$

ainsi, d'après P3, on a bien $|F'(y)| = |F'(x)|$.

Ensuite, la formule de Taylor à l'ordre 2 appliquée à F, i.e. $F(X+Y) - F(X) - YF'(X) = Y^2 G(X,Y)$ avec $G \in A[X,Y]$, assure l'existence de $\beta \in A$ tel que :

$$F(y) = F(x) - \frac{F(x)}{F'(x)}F'(x) + \beta\left(\frac{F(x)}{F'(x)}\right)^2 = \beta\left(\frac{F(x)}{F'(x)}\right)^2,$$

si bien que :

$$|F(y)| \leqslant \left|\frac{F(x)}{F'(x)}\right|^2.$$

Ainsi :

$$\rho_y = \left|\frac{F(y)}{F'(y)^2}\right| = \left|\frac{F(y)}{F'(x)^2}\right| \leqslant \left|\frac{F(x)^2}{F'(x)^4}\right| = \rho_x^2,$$

ce qu'il fallait montrer. $\square$

Avant de passer à l'application principale du lemme 8, nous allons établir le lemme :

Lemme 9 (Séparation des racines) *Soit K un corps muni d'une valeur absolue* ***ultra-métrique*** *$|\ |$, A l'anneau de valuation pour K associé à $|\ |$. On considère F un polynôme de $A[X]$ et r une racine* ***entière*** *de F (i.e. $r \in A$). Soit $r' \in K$ une autre racine de F ; si $|r - r'| < |F'(r)|$ alors $r = r'$.*

> **Remarque** – On a le même résultat avec $x, y \in A \times K$ tels que $F(x) = F(y)$ et $|x - y| < |F'(x)|$. Il suffit en effet d'appliquer le lemme de séparation des racines au polynôme $G = F - F(x)$.

Preuve — Commençons par remarquer que r' est entière. En effet, la racine r l'étant, nécessairement $|F'(r)| \leqslant 1$. Par conséquent, $|r - r'| \leqslant 1$, ou encore $r - r' \in A$, ce qui entraîne $r' \in A$ (car r a été supposée entière). Cela étant, introduisons l'idéal $I = \{a \in A,\ |a| < |F'(r)|\}$ alors $r \equiv r' \pmod I$. Ecrivons $F(r') - F(r) = (r' - r)Q(r, r')$ avec $Q \in A[X,Y]$ vérifiant $Q(X,X) = F'(X)$. Nous allons montrer que $Q(r,r') \neq 0$ et cela suffira pour conclure. Remarquons que :

$$Q(r, r') \equiv Q(r, r) \equiv F'(r) \mod I.$$

Mais, par définition de l'idéal I, $F'(r) \notin I$, i.e. $F'(r) \not\equiv 0 \mod I$; nécessairement $Q(r, r') \neq 0$. $\square$

Nous utiliserons ce lemme à de nombreuses reprises dans la suite, comme d'ailleurs dans le résultat suivant :

Corollaire 8 *Soit K un corps* ***complet*** *pour une valeur absolue ultra-métrique $|\ |$. On note A l'anneau de valuation pour K associé à $|\ |$ et on considère $F \in A[X]$. Soit $x \in A$ tel que :*

$$|F(x)| < |F'(x)^2| \tag{$*$}$$

alors la suite $(x_k)_k$ définie par :

$$x_0 = x \qquad et \qquad x_{k+1} = x_k - \frac{F(x_k)}{F'(x_k)} \quad \forall k \geqslant 0,$$

converge vers une racine r de F dans A telle que :

$$|r - x| \leqslant \left|\frac{F(x)}{F'(x)}\right|.$$

En conséquence, $|r - x| < |F'(x)|$ et r est l'unique racine de F (dans une clôture algébrique de K) à vérifier cette dernière.

Preuve — La preuve consiste à remarquer que la construction de Newton du lemme 8 peut se réitérer. D'après le lemme 8, si y est l'itéré de Newton de x alors il vérifie aussi les hypothèses de ce lemme. En effet, pour ce faire, il faut que y satisfasse à l'inégalité $|F(y)| < |F'(y)^2|$ ou encore avec une notation déjà introduite $\rho_y < 1$. Mais comme on a montré que $\rho_y \leqslant \rho_x^2$, on a bien $\rho_y < 1$ (car $\rho_x < 1$ par hypothèse). Le procédé de Newton se réitère donc et on peut construire la suite $(x_k)_k$ du corollaire. En vertu du lemme 8, cette dernière vérifie :

$$|F'(x_k)| = |F'(x_{k-1})| = |F'(x_0)| \qquad \text{et} \qquad \rho_k \leqslant \rho_{k-1}^2 \leqslant \rho_0^{2^k} \quad \text{avec} \quad \rho_k = \rho_{x_k}.$$

Notons C la valeur commune des $|F'(x_k)|$, alors on a :

$$|x_k - x_{k-1}| = C\rho_{k-1}, \quad |F(x_k)| = C^2\rho_k \quad \text{et} \quad |x_k - x| \leqslant C\rho_0.$$

La première égalité montre que la suite (x_k) est de Cauchy (car ρ_k tend vers zéro). Elle converge donc car K est complet. Notons r sa limite. La deuxième égalité prouve que r est une racine de F. Enfin, grâce à la dernière inégalité, on établit que :

$$|r - x| \leqslant C\rho_0 = \left|\frac{F(x)}{F'(x)}\right|.$$

Il reste à vérifier la propriété d'unicité ; dans le corps K, c'estune conséquence directe du lemme 9. En effet, si r' est une autre racine de F vérifiant :

$$|r' - x| \leqslant \left|\frac{F(x)}{F'(x)}\right|,$$

alors comme $|F(x)| < |F'(x)^2|$, on a en fait :

$$|r - x| < |F'(x)| \quad \text{et} \quad |r' - x| < |F'(x)| \qquad \text{donc} \qquad |r - r'| < |F'(x)|.$$

Mais d'après P3, $|F'(x)| = |F'(r)|$; ainsi, on a en fait :

$$|r - r'| < |F'(r)|,$$

d'où $r = r'$ d'après le lemme 9.

Pour montrer l'unicité dans une clôture algébrique de K, il faut, de plus, utiliser l'existence et l'unicité du prolongement de la valeur absolue à toute extension algébrique de K. Ensuite, il suffit de réitérer le raisonnement précédent. □

Remarque – Cette proposition figure dans [14] (Chap XII, §7, Proposition 7.6), cependant, il y est simplement vérifié que $|r - x| \leqslant \left|\frac{F(x)}{F'(x)^2}\right|$. Cette majoration ne suffit pas pour montrer que la racine r est unique. En revanche, dans [16], la proposition est énoncée comme précédemment. Pourtant il n'y est pas question d'unicité.

Traitons un cas particulier très répandu dans la littérature :

Corollaire 9 *Soit* $(K, |\ |)$ *un corps ultra-métrique complet,* A *l'anneau de valuation pour* K *associé à* $|\ |$ *et* $\mathfrak{m}$ *son idéal maximal. Tout polynôme* $F \in A[X]$ *admettant une racine* x ***simple*** *modulo* $\mathfrak{m}$*, admet une racine* r *dans* A *vérifiant* $|r - x| < 1$ *i.e.* $r \equiv x \pmod{\mathfrak{m}}$*. De plus, cette racine est unique dans une clôture algébrique de* K*.*

Preuve — Puisque x est une racine simple modulo $\mathfrak{m}$, on a $|F(x)| < 1$ et $|F'(x)| = 1$, ce qui permet de conclure en appliquant le corollaire 8. □

Plus généralement, on peut, d'ores et déjà, montrer un autre résultat. En fait ce dernier est une conséquence directe du lemme de Hensel dont il sera question dans la section IV. Notons que la démonstration proposée ci-après utilise le prolongement (unique) de la valeur absolue d'un corps ultra-métrique complet à toute extension algébrique, alors que la preuve consistant à utiliser le lemme de Hensel s'en passe. Cette remarque ne figure ici que dans un soucis de cohérence ; en effet, le lemme de Hensel peut être utilisé dans la preuve du prolongement de la valeur absolue d'un corps ultra-métrique complet...

Corollaire 10 *Soit* $(K, |\ |)$ *un corps ultra-métrique complet,* A *l'anneau de valuation pour* K *associé à* $|\ |$*, dont on note* $\mathfrak{m}$ *l'idéal maximal et* k *le corps résiduel. Si* $F \in A[X]$ *est un polynôme unitaire et séparable modulo* $\mathfrak{m}$*, alors les facteurs irréductibles de* F *dans* $A[X]$ *sont en correspondance bijective avec ceux de* $\overline{F}$ *(qui désigne la classe de* F *modulo* $\mathfrak{m}$*) dans* $k[X]$*.*

Plus précisément, si $F = F_1 \cdots F_k$ *est la décomposition de* F *en irréductibles (unitaires) de* $A[X]$ *alors* $\overline{F} = \overline{F_1} \cdots \overline{F_k}$ *est celle de* $\overline{F}$ *dans* $k[X]$*.*

Preuve — Soit G un diviseur irréductible unitaire de F dans $A[X]$. On considère $h \in k[X]$ un diviseur irréductible de $\overline{G}$ dont on note H un représentant unitaire dans $A[X]$ (H est nécessairement irréductible et $\deg H \leqslant \deg G$). Plaçons nous désormais dans le corps $L = K(x)$ où x est une racine de H et notons l le corps résiduel de L. Par construction, G admet donc une racine modulo $\mathfrak{m}$; cette dernière est simple puisque G divise F qui est séparable modulo $\mathfrak{m}$, par hypothèse. Par conséquent, d'après le corollaire 9, G admet une racine dans L. Par conséquent, $\deg G \leqslant \deg H$ ce qui implique que $\deg G = \deg H = \deg h$. Ainsi $\overline{G} = h$, ou encore G reste irréductible modulo $\mathfrak{m}$. □

III.2 Illustration dans le cadre des corps locaux corps rsiduel fini

Dans cette section, nous nous intressons aux corps locaux **corps rsiduel fini** ; cela quivaut au fait qu'ils soient **localement compacts**. En effet, un rsultat classique de la thorie des valuations (c.f. [3], Chap 6, §5, n°1, Proposition 2) affirme que pour qu'un corps K muni d'une valuation v (non triviale) soit localement compact, il faut et il suffit que les trois conditions suivantes soient vrifies :

1. K est complet ;
2. v est discrte ;
3. le corps rsiduel de K (associ v) est fini.

III.2.1 Structure des corps locaux corps rsiduel fini

Nous allons montrer, en guise d'illustration de la mthode de Newton, le rsultat suivant :

Théorème 9 *Soit* K *un corps ultra-mtrique complet, corps rsiduel,* k*, fini de cardinal* q *; on note* A *l'anneau de valuation pour* K *et* $\mathfrak{m}$ *son idal maximal.*

(i) Le polynme $X^q - X$ *est sparable et totalement scind sur* K *; on note* R *l'ensemble de ses racines :*

$$R = \{x \in K,\ x^q = x\} = \{x \in A,\ x^q = x\}$$

L'ensemble R *est de cardinal* q *et* $R = \mathbb{U}_{q-1} \cup \{0\}$*, o* $\mathbb{U}_{q-1}$ *dsigne le groupe des racines* $(q-1)$*-mes de l'unit.*

(ii) L'anneau A *est le runion* ***disjointe*** *des boules* ***ouvertes*** *de rayon* 1 *de centre un point de* R*.*

(iii) On dispose d'une section canonique $k \to R$ *qui un lment* $\xi \in k$ *associe l'unique* $x \in R$ *tel que :* $\overline{x} = \xi$ *; on dfinit ainsi une application* $r : A \to R$ *telle que : pour* $x \in A$*,* $r(x)$ *est l'unique lment de* R *vrifiant :* $x \equiv r(x) \pmod{\mathfrak{m}}$*.*

(iv) La rduction modulo $\mathfrak{m}$ *:* $\mathbb{U}_{q-1} \to k^*$*, induit un isomorphisme de groupes (cycliques).*

(*v*) *Pour tout* $x \in A$*, on a :*
$$\lim_{n\to\infty} x^{q^n} = r(x)$$

(*vi*) *Supposons de plus K* ***local*** *; alors si* π *est une uniformisante de A, tout lment de A s'crit de manire unique sous la forme d'une srie convergente :*

$$x = x_0 + x_1\pi + \cdots + x_n\pi^n + \cdots , \qquad x_i \in R$$

Les proprits de ce thorme se "lisent" assez naturellement dans le cas particulier $K = k((X))$, $A = k[[X]]$, $\mathfrak{m} = Xk[[X]]$ (o k est un corps fini de cardinal q). On dispose dans cet exemple-ci d'une section canonique $s : k \to A$ de la rduction modulo $\mathfrak{m}$ savoir l'application qui tout lment $\xi \in k$ associe la srie formelle constante de terme constant gal ξ (le fait que k soit fini n'est d'aucune importance pour le moment). L'application r n'est rien d'autre que l'application qui associe, toute srie formelle, S, son terme constant, $S(0)$; on sait bien que $S(0)$ est l'unique lment de k tel que $S \equiv S(0) \pmod{X}$. Enfin, pour $S \in k[[X]]$,

$$S = S(0) + a_1X + \cdots + a_kX^k + \cdots , \quad \text{on a :} \quad S^{q^n} = S(0) + a_1X^{nq} + \cdots + a_kX^{knq} + \cdots ;$$

les puissances de X sont "chasses" l'infini, autrement dit, $\lim_{n\to\infty} S^{q^n} = S(0)$.

Cela tant, avant de faire la preuve du rsultat prcdent, nous allons montrer un lemme :

Lemme 10 *Sous les hypothses du thorme prcdent, si* $x, y \in A$ *vrifient* $y - x \in \mathfrak{m}^k$ *avec* $k \geqslant 1$*, alors pour tout* $n \geqslant 0$*,* $y^{q^n} - x^{q^n} \in \mathfrak{m}^{k+n}$*.*

Preuve — Par rcurrence sur n, on se ramne au cas $n = 1$. On remarque que $x \equiv y \pmod{\mathfrak{m}}$ et on crit :

$$y^q - x^q = (y - x)(\text{somme de } q \text{ termes deux deux congrus modulo } \mathfrak{m})$$

Mais comme $\#k = q$, une somme de q termes deux deux congrus modulo $\mathfrak{m}$ appartient encore $\mathfrak{m}$ (raisonner modulo $\mathfrak{m}$), d'o le rsultat. □

Preuve du thorme 9 — (*i*) Notons $F(X) = X^q - X$. Puisque $\#k = q$, le polynme F est sparable et totalement scind modulo $\mathfrak{m}$. Ainsi, en vertu du corollaire 10, F est aussi sparable et totalement scind sur K.

(*ii*) Soit $x \in A$, comme $\#k = q$, on a $x^q \equiv x \pmod{\mathfrak{m}}$, i.e. $|F(x)| = |x^q - x| < 1$. Autrement dit, x est une racine (simple) de F modulo $\mathfrak{m}$. Par consquent, il existe une unique racine $r \in R$ de F telle que $|r - x| < 1$. Cela montre bien que :

$$A = \bigvee_{r\in R} \mathcal{B}(r, 1)$$

o $\mathcal{B}(r, 1)$ dsigne la boule ouverte de centre r et de rayon 1.

Les propits (*iii*) et (*iv*) ne posant aucun problme, passons l'avant-dernier point : pour commencer, on remarque que si cette suite converge, alors sa limite l, vrifie bien $l^q = l$, c'est dire $l \in R$ et $|l - x| < 1$, c'est dire $l = r(x)$; en effet, la valeur absolue tant ultra-mtrique,

$$|x^{q^n} - x| < 1, \ \forall n \geqslant 0 \qquad \text{implique :} \qquad \left|\lim_{n\to\infty} x^{q^n} - x\right| = |l - x| < 1$$

Il reste montrer que la suite $(x^{q^n})_n$ converge. Il suffit de vrifier qu'elle est de Cauchy, ou encore :

$$\lim_{n\to\infty} x^{q^{n+1}} - x^{q^n} = 0$$

Cela dcoule directement du lemme 10 appliqu $x = x$ et $y = x^q$; en effet on montre ainsi :

$$x^{q^{n+1}} - x^{q^n} \in \mathfrak{m}^{n+1}$$

d'o la conclusion. □

III.2.2 Paramtrisation des extensions de corps locaux

Etant donns p un premier de $\mathbb{Z}$, e et f deux entiers positifs (strictement), le but de cette section est d'exhiber un polynme $F \in \mathbb{Z}_p[X]$ irrductible dans $\mathbb{Z}_p[X]$ tel que le corps p-adique engendr par une racine θ de F vrifie la condition :

$$e(\mathbb{Q}_p(\theta)/\mathbb{Q}_p) = e \qquad \text{et} \qquad f(\mathbb{Q}_p(\theta)/\mathbb{Q}_p) = f \tag{e,f}$$

Dans la suite, on dsignera une telle extension par (e, f) $\mathbb{Q}_p$-extension.

Pour commencer, nous allons nous attacher dcrire les extensions non ramifies des corps locaux corps rsiduels finis (i.e. localement compact). Les deux rsultats suivants sont classiques (ils figurent en particulier dans [17], [13], ou encore [10]) ; nous les faisons figurer ici pour illustrer une nouvelle fois la mthode de Newton.

Proposition 30 *Soit K un corps local corps rsiduel, k, fini d'ordre q. On considre un entier $m \geqslant 1$ premier avec q ; alors l'extension $K(\mathbb{U}_m)/K$ est non ramifie de degr l'ordre de q dans $U(\mathbb{Z}/m\mathbb{Z})$.*

Preuve — Soit $m \geqslant 1$ un entier premier avec q. Modulo q, le m-me polynme cyclotomique, Φ_m, est sparable et se factorise en irrductibles tous de mme degr, savoir, f, l'ordre de q dans $\mathrm{U}(\mathbb{Z}/m\mathbb{Z})$. D'aprs le corollaire 10, Φ_m est donc produit de $\varphi(m)/f$ irrductibles de degr f dans $K[X]$. Ainsi, toute racine m-me de l'unit, ξ, est de degr f sur K et l'extension $K(\xi)/K$ est non ramifie car le polynme minimal de ξ sur K reste irrductible dans k. □

Corollaire 11 *Soit K un corps local corps rsiduel, k, fini d'ordre q. Pour tout entier $f \geqslant 1$, il existe une K-extension non ramifie de degr f ; de plus, une clture algbrique de K tant fixe, isomorphisme prs, cette extension est unique. On la note K_f.*

Plus prcisment, pour tout entier $m \geqslant 1$, premier avec q et tel que q soit d'ordre f dans $U(\mathbb{Z}/m\mathbb{Z})$, on a : $K_f = K(\mathbb{U}_m)$. En particulier, $K_f = K(\mathbb{U}_{q^f-1})$.

Preuve — Immdiat une fois que l'on a remarqu qu'en particulier $K_f = K(\mathbb{U}_{q^f-1})$. □

De la mme manire, les extensions totalement ramifies de corps locaux sont caractrises par leurs lments primitifs. On peut montrer le rsultat suivant (c.f. [17], Chap 5, §2, n°2, ou [13], Chap II, §5) :

Proposition 31 *Soit L/K une extension (finie) totalement ramifie de corps locaux, alors toute uniformisante de L est un lment primitif de cette extension dont le polynme minimal (sur K) est un polynme d'Eisenstein (pour le premier de K).*

Rciproquement, toute extension de K engendre par une racine d'un polynme d'Eisenstein est totalement ramifie.

De plus, dans chacun des deux cas prcdents (i.e. extensions non ramifies et totalement ramifies), les lments primitifs mis en avant sont aussi monognes pour les anneaux d'entiers sous-jacents. Autrement dit leurs polynmes minimaux vrifient le critre de Dedekind. On peut, chaque fois le redmontrer " la main" sans invoquer le critre prcdent. Pour finir, propos des extensions de corps locaux, montrons que :

Proposition 32 *Soit K un corps local corps rsiduel, k, fini de cardinal q et L/K une extension finie ; $\mathcal{O}_K$ et $\mathcal{O}_L$ dsignent les anneaux d'entiers respectifs de K et L. Introduisons L_0 la sous K-extension non ramifie maximale contenue dans L, f le degr de L_0/K (i.e. $f = f(L/K)$), x un lment primitif de l'extension L_0/K tel que $x^{q^f} = x$ et enfin y une uniformisante de l'extension L/L_0 ; alors $x + y$ engendre l'extension L/K et vrifie :*

$$\mathcal{O}_L = \mathcal{O}_K[x + y]$$

En particulier, l'extension d'anneaux $\mathcal{O}_K \subset \mathcal{O}_L$ est monogne.

Preuve — Un petit schma pour commencer :

$$K \overbrace{\qquad\qquad\qquad\qquad}^{\text{non ramifie}} L_0 = K(x) \overbrace{\qquad\qquad\qquad\qquad}^{\text{tot. ramifie}} L = L_0(y) = K(x, y)$$

On sait, de plus, que x et y sont des lments monognes des anneaux d'entiers des corps qu'ils engendrent ; autrement dit, avec des notations implicites :

$$\mathcal{O}_{L_0} = \mathcal{O}_K[x], \quad \mathcal{O}_L = \mathcal{O}_{L_0}[y] \qquad \text{donc} \qquad \mathcal{O}_L = \mathcal{O}_K[x, y]$$

Nous allons en fait tablir que $\mathcal{O}_K[x,y] = \mathcal{O}_K[x+y]$. Bien sr, $\mathcal{O}_K[x+y] \subset \mathcal{O}_K[x,y]$; mieux, $\mathcal{O}_K[x+y]$ est ferm dans $\mathcal{O}_K[x,y] = \mathcal{O}_L$ (c'est un sous $\mathcal{O}_K$-module libre de rang fini). Il suffit, par exemple, de montrer que $x \in \mathcal{O}_K[x+y]$. Or y est une uniformisante de L, et x est une racine (q^f-1)-me de l'unit. Par consquent, grce au thorme 9 (dont on reprend les notations) appliqu au corps L, on dduit : $r(x+y) = x$; mais $r(x+y)$ est aussi la limite de la suite $(x+y)^{q^n}$ qui appartient $\mathcal{O}_K[x+y]$ (cet ensemble tant ferm). Ainsi, $x \in \mathcal{O}_K[x+y]$, d'o le rsultat. $\square$

Application la paramtrisation des extensions de $\mathbb{Q}_p$

Soit p un premier de $\mathbb{Z}$ et e, f deux entiers (strictement) positifs. On cherche $F \in \mathbb{Z}_p[X]$ dont une racine engendre une (e,f) $\mathbb{Q}_p$-extension.

Un petit intermde polynomial : soient P et Q deux polynmes unitaires de degr m et n coefficients dans un anneau A intgre (et commutatif !) ayant pour racines dans une extension $x_1, \ldots, x_m$ et $y_1, \ldots, y_n$. Alors, la A-algbre :

$$A[X,Y]/\langle P(X), Q(Y)\rangle \simeq A[X]/\langle P(X)\rangle \otimes_A A[Y]/\langle Q(Y)\rangle$$

admet les $(x^i y^j)_{\substack{0 \leqslant i \leqslant n-1 \\ 0 \leqslant j \leqslant m-1}}$ comme A-base (o on a pos $x = \overline{X}$ et $y = \overline{Y}$). C'est donc une A-algbre libre dans laquelle la notion de polynme caractristique (entre autre) est bien dfinie. En particulier, pour tout $\lambda \in A$, on peut considrer le polynme caractristique de $y + \lambda x$, not $P \oplus_\lambda Q$; il est unitaire, coefficients dans A, de degr mn et se calcule comme suit :

$$P \oplus_\lambda Q = \mathrm{res}_Y(P(Y), Q(Y - \lambda X))$$

Tout d'abord, considrons $I \in \mathbb{Z}_p[X]$ un polynme unitaire de degr f irrductible modulo p, et $E \in \mathbb{Z}_p[X]$ est un polynme d'Eisenstein (pour le premier p) de degr e. Si x et y sont deux racines respectives de I et E, alors l'extension $\mathbb{Q}_p(x,y)/\mathbb{Q}_p$ est une (e,f) $\mathbb{Q}_p$-extension. En effet, compte tenu des rsultats prcdents, on a :

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q}_p(x,y) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}_p(x) \arrow[dr, dash, "f", "\mathrm{nr}"'] & & \mathbb{Q}_p(y) \arrow[dl, dash, "e"', "\mathrm{tr}"] \\
 & \mathbb{Q}_p &
\end{tikzcd}$$

Les extensions $\mathbb{Q}_p(x)/\mathbb{Q}_p$ et $\mathbb{Q}_p(y)/\mathbb{Q}_p$ tant respectivement non ramifie et totalement ramifie sur $\mathbb{Q}_p$, elles sont linairement disjointes sur $\mathbb{Q}_p$. Par consquent, l'extension $\mathbb{Q}_p(x,y)/\mathbb{Q}_p$ est de degr ef ; on en dduit facilement qu'elle vrifie les caractristiques voulues. De plus, sauf pour un nombre fini de $\lambda \in \mathbb{Z}$, l'lment $y + \lambda x$ est primitif. Par suite, le polynme $I \oplus_\lambda E$ est son polynme minimal sur $\mathbb{Q}_p$ (car il est de degr ef) ; il convient donc ...

Remarques

1. Rien ne nous empche dans la construction prcdente de ne considrer que des polynmes coefficients entiers ; on obtient ainsi, un polynme comme on le souhaite, mais de surcrot coefficients entiers.

2. Quand bien mme on permet aux polynmes de la construction prcdente d'tre coefficients p-adiques, on ne pourra pas obtenir ainsi **toutes** les (e,f) $\mathbb{Q}_p$-extensions. Par exemple, l'une des trois extensions quadratiques (c.f. [17], pour ce qui concerne les extensions quadratiques des corps p-adiques) de K_2 l'unique extension non ramifie de $\mathbb{Q}_p$ (p premier **impair**) de degr 2, savoir $K_2(\sqrt{p\xi})$ o ξ est une racine (primitive) (p^2-1)-me de l'unit, ne sera jamais "atteinte". Pour s'en convaincre, il suffit d'numrer les extensions totalement ramifies de $\mathbb{Q}_p$ de degr 2 et d'examiner leurs compositums avec K_2.

Grce la proposition 32, nous allons pouvoir nous dbarasser du paramtre λ. Soit $m \geqslant 1$ un entier tel que p soit d'ordre f dans $\mathrm{U}(\mathbb{Z}/m\mathbb{Z})$ et I un facteur irrductible (dans $\mathbb{Z}_p[X]$) du m-me polynme cyclotomique Φ_m. On sait que ce facteur est de degr f et qu'une quelconque de ses racines engendre une $\mathbb{Q}_p$-extension non ramfie de degr f. Soit maintenant $E \in \mathbb{Z}_p[X]$ un polynme d'Eisenstein (pour p) de degr e. Alors le polynme $I \oplus_1 E$ est irrductible de degr ef et une quelconque de ses racines engendre une extension de $\mathbb{Q}_p$ avec les caractristiques voulues. En effet, soit θ une racine de $I \oplus_1 E$. Par construction, il existe x racine de I et y racine de E telles que $\theta = x + y$. Mais x vrifie $x^{p^f} = x$ et y est une uniformisante de $\mathbb{Q}_p(x,y)$, par suite $x + y$ engendre, d'aprs la proposition 32, l'extension $\mathbb{Q}_p(x,y)/\mathbb{Q}_p$.

Contrairement la construction prcdente, le polynme obtenu peut tre "fortement p-adique" ; plus prcisment, le polynme I n'a aucune raison d'tre coefficients entiers. Il l'est si Φ_m reste irrductible dans $\mathbb{Z}_p[X]$, c'est dire si p engendre $\mathrm{U}(\mathbb{Z}/m\mathbb{Z})$. C'est le cas, par exemple, pour $p = 2$, $m = 9$; en effet, 2 est d'ordre $\varphi(9) = 6$ dans $\mathrm{U}(\mathbb{Z}/9\mathbb{Z})$. Par suite, quelque soit $E \in \mathbb{Z}[X]$ d'Eisenstein de degr e, le polynme $\Phi_m \oplus_1 E$, de degr $6e$, est irrductible sur $\mathbb{Q}_2$ et une quelconque de ses racines engendre une $(e, 6)$ $\mathbb{Q}_2$-extension.

Plus gnralement, soit $m \geqslant 1$ un entier tel que le groupe des inversibles $\mathrm{U}(\mathbb{Z}/m\mathbb{Z})$ soit cyclique (ce qui est quivalent $m \in \{2, 4, q^\alpha, 2q^\alpha\}$ o q est un premier impair, c.f. [18], Chap IV, exercice 18). D'aprs le thorme de Dirichlet, il existe une infinit de premiers qui engendrent ce groupe. Pour p un quelconque des ces derniers, si E est un polynme d'Eisenstein (pour p) de degr e alors une quelconque racine de $\Phi_m \oplus_1 E$ engendre une $(e, \varphi(m))$ $\mathbb{Q}_p$-extension (donc de degr $\varphi(m)e$).

Ainsi toute racine de $\Phi_9 \oplus_1 E$ engendre une $(e, 6)$ extension sur $\mathbb{Q}_2$, $\mathbb{Q}_5$, $\mathbb{Q}_{11}$, $\mathbb{Q}_{23}$, $\mathbb{Q}_{29}$ ... Dans le mme ordre d'ide, $\Phi_{50} \oplus_1 E$ fournit des $(e, 20)$ extensions de $\mathbb{Q}_3$, $\mathbb{Q}_{13}$, $\mathbb{Q}_{17}$, $\mathbb{Q}_{23}$ ...

III.2.3 Un résultat dû à Stickelberger

Nous donnons ici une ultime application de la méthode de Newton. Nous en profiterons pour, une nouvelle fois, illustrer le principe de localisation et globalisation.

Proposition 33 *Soit K un corps local à corps résiduel, k, fini de cardinal q impair. Alors pour tout $x \in U(K)$ (c'est à dire inversible dans l'anneau des entiers de K), on a :*

$$\left(\frac{x}{K}\right) = \left(\frac{\overline{x}}{\mathbb{F}_q}\right)$$

où $\overline{x}$ désigne, la classe de x modulo l'idéal maximal de l'anneau des entiers de K.

Preuve — Si x est un carré dans le corps K, il est évident que modulairement, il vérifie encore cette propriété. Pour la réciproque, on considère le polynôme $F(X) = X^2 - x$. Il admet une racine dans k par hypothèse. Cette racine est simple car on a supposé $x \in \mathrm{U}(K)$ et q impair. En vertu du corollaire 9, F admet une racine dans K d'où la conclusion. $\square$

Remarque – Il est indispensable de supposer $x \in \mathrm{U}(K)$; en effet, si π est une uniformisante de K, alors π étant irréductible, on a $\left(\frac{\pi}{K}\right) = -1$ alors que $\left(\frac{\pi}{q}\right) = \left(\frac{0}{q}\right) = 1$.

Grâce à ce résultat, on peut démontrer "simplement" un critère dû à Stickelberger (que l'on trouve énoncé dans [7], Chap 4, §8, Proposition 4.8.10) liant le caractère quadratique du discriminant d'un corps de nombres, K, modulo un premier p de $\mathbb{Z}$ non ramifié dans K et le nombre d'idéaux premiers de K au dessus de p.

Dans la preuve proposée, où nous "localisons", interviennent les discriminants de corps p-adiques. Le discriminant d'un corps p-adique est un idéal de $\mathbb{Q}_p$ dont les générateurs sont égaux au carré d'un inversible près. Ainsi, les générateurs de l'idéal discriminant ont tous le même caractère quadratique. Tout ça pour dire, qu'étant donné E un corps p-adique, on peut donner un sens à la notation :

$$\left(\frac{\operatorname{dis} E}{\mathbb{Q}_p}\right)$$

ce nombre est égal à 1 si et seulement si un des générateurs de l'idéal $\operatorname{dis}(E)$ est un carré dans $\mathbb{Q}_p$.

Cela étant, montrons désormais que :

Proposition 34 (Stickelberger) *Soit K un corps de nombres de degré n et p un premier impair **non ramifié** dans K : $\langle p \rangle = \mathfrak{p}_1 \cdots \mathfrak{p}_g$. Alors :*

$$\left(\frac{\operatorname{dis} K}{p}\right) = (-1)^{n-g}$$

Preuve — Comme p est non ramifié dans K, p est premier avec $\operatorname{dis}(K)$. Par conséquent, d'après la proposition 33 :

$$\left(\frac{\operatorname{dis} K}{p}\right) = \left(\frac{\operatorname{dis} K}{\mathbb{Q}_p}\right)$$

Ecrivons :

$$\operatorname{dis}(K) = \prod_{i=1}^{g} \operatorname{dis}(K_i) \qquad \text{où :} \quad K_i = K_{\mathfrak{p}_i}$$

Si $n_i = [K_i : \mathbb{Q}_p]$ alors $n = \sum n_i$; de plus, l'extension $K_i/\mathbb{Q}_p$ est non ramifiée donc cyclique. Ainsi, $\left(\frac{\operatorname{dis} K_i}{\mathbb{Q}_p}\right) = (-1)^{n_i - 1}$. Mais de nouveau, $\left(\frac{\operatorname{dis} K_i}{p}\right) = \left(\frac{\operatorname{dis} K_i}{\mathbb{Q}_p}\right)$ donc :

$$\left(\frac{\operatorname{dis} K}{p}\right) = \left(\frac{\operatorname{dis} K_1}{p}\right) \cdots \left(\frac{\operatorname{dis} K_g}{p}\right) = (-1)^{\sum (n_i - 1)} = (-1)^{n-g}$$

ce que l'on voulait. □

III.3 Proximité au sens de Serre et au sens de Krasner

Un des résultats classiques de la théorie des corps complets pour une valeur absolue ultra-métrique est connu sous le nom de lemme de Krasner (c.f. [13], ou [17], ou encore la fin de cette section). Il y est question d'une certaine "proximité" que nous allons lier à la méthode de Newton. Nous dégagerons en fait deux types de "proximité".

Avant toute chose, notons que dans tout ce qui suit nous allons utiliser (de façon peut être insidieuse) l'unicité du prolongement de la valeur absolue ultra-métrique d'un corps complet à toute extension algébrique de ce corps, alors que la méthode de Newton ne l'utilisait pas (hormis pour l'unicité dans une clôture algébrique). Cela étant, dans tout ce qui suit, K est un corps ultra-métrique complet dont on fixe une clôture algébrique.

Pour commencer, considérons $F \in K[X]$ un polynôme et x algébrique sur K qui n'annule pas la dérivée de F. On appelle $\mathcal{R}$ l'ensemble des racines de F (dans la clôture algébrique de K précédemment fixée). Parmi les racines de F, choisissons $r \in \mathcal{R}$ de façon à minimiser $|r - x|$ i.e. $|x - r| = \min\{|x - s|,\ s \in \mathcal{R}\}$. Nous allons montrer que $|x - r| \leqslant \frac{|F(x)|}{|F'(x)|}$ ou encore $|x - r||F'(x)| \leqslant |F(x)|$. Pour $r' \in \mathcal{R}$, on note $\Pi_{r'}$ la quantité définie par :

$$\Pi_{r'} = \prod_{s \in \mathcal{R} \setminus \{r'\}} |x - s|.$$

Alors compte tenu du choix de r, quelque soit $r' \in \mathcal{R}$, $\Pi_{r'} \leqslant \Pi_r$. Par conséquent, grâce à l'"ultra-métricité" de la norme, on montre que $|F'(x)| \leqslant |a|\Pi_r$ où a est le coefficient dominant de F. Ainsi,

$$|x - r||F'(x)| \leqslant |a||x - r|\Pi_r = |F(x)| \qquad \text{et donc} \qquad |x - r| \leqslant \frac{|F(x)|}{|F'(x)|},$$

ce que l'on voulait.

Ainsi, si on suppose de plus que x est entier sur A et que $|F(x)| \leqslant |F'(x)|$, alors le raisonnement précédent montre de plus que r est entier. Sans rapport avec ce qui précède, je rappelle un résultat classique de théorie des corps auquel nous ferons appel dans la suite :

Lemme 11 *Soit K un corps. Un élément x, algébrique sur K, est séparable sur K si et seulement s'il est racine d'un polynôme $F \in K[X]$ vérifiant $F'(x) \neq 0$.*

Preuve — Soit G le polynôme minimal de x sur K ; il divise F : $F = GH$. Ainsi, $F' = G'H + GH'$ donc $F'(x) = G'(x)H(x) \neq 0$. Nécessairement, $G'(x) \neq 0$; a fortiori $G' \neq 0$ donc G est séparable car irréductible (un polynôme irréductible est séparable si et seulement si sa dérivée est non nulle). □

Nous pouvons désormais établir une proposition qui est l'analogue du corollaire 8. Nous donnons, volontairement, pour bien distinguer la différence d'état d'esprit des deux méthodes, un énoncé où le prolongement unique de la valeur absolue est très sous-jacent :

Proposition 35 (Newton sans la méthode de Newton) *Soit K un corps* ***complet*** *pour une valeur absolue ultra-métrique $|\ |$. On note A l'anneau de valuation pour K associé à $|\ |$ et on considère F un polynôme de $A[X]$. Soit x un élément entier sur A tel que :*

$$|F(x)| < |F'(x)^2|,$$

alors le polynôme F admet une racine $r \in K(x)$ vérifiant $|r - x| < |F'(x)|$; de plus, cette racine est unique dans une clôture algébrique de K.

Preuve — Pour l'unicité, on commence par remarquer que la racine r est nécessairement entière sur A ; en effet, x étant entier, on a $|F'(x)| \leqslant 1$, de sorte que $|r-x| \leqslant 1$. Ainsi, $r-x$ est entier sur A, d'où le même résultat pour la racine r. De plus, comme $|x-r| < |F'(x)|$, on sait, grâce à P3 que $|F'(x)| = |F'(r)|$. Par suite, si r' est une autre racine de F vérifiant $|x-r'| < |F'(x)|$, alors

$$|r-r'| \leqslant \max\{|r-x|, |r'-x|\} < |F'(x)| = |F'(r)| \ ;$$

donc $r = r'$ en vertu du lemme de séparation des racines (lemme 9) appliqué dans une extension "assez grande" de K.

Pour l'existence, comme précédemment, on introduit $\mathcal{R}$ l'ensemble des racines de F (dans une clôture algébrique de K fixée). Parmi les racines de F, on choisit $r \in \mathcal{R}$ de façon à minimiser $|r-x|$ i.e. $|x-r| = \min\{|x-s|,\ s \in \mathcal{R}\}$. Alors, nous l'avons déjà montré :

$$|x-r| \leqslant \frac{|F(x)|}{|F'(x)|} < |F'(x)|$$

En conséquence, nécessairement r est entier comme nous avons déjà pu le constater. Nous allons utiliser cette remarque pour montrer que $r \in K(x)$. Nous aurons besoin pour cela de vérifier que r est la seule racine de F à minimiser la quantité $|x-r|$. Si une deuxième racine r' de F vérifie cette propriété alors en particulier $|x-r| = |x-r'|$ de telle sorte que $|r-r'| < |F'(x)|$ (et r' est elle aussi entière). En outre, nous savons que $|F'(x)| = |F'(r)|$, par conséquent, d'après le lemme de séparation des racines (lemme 9), $r = r'$ ce qui est contradictoire. Ainsi, r vérifie bien :

$$|x-r| < |x-s| \quad \forall s \in \mathcal{R} \setminus \{r\}.$$

Enfin, remarquons que nécessairement $|F'(x)| \neq 0$. Par suite, comme $|F'(x)| = |F'(r)|$, on a $F'(r) \neq 0$, ce qui entraîne, en vertu du lemme 11, que r est séparable sur K

La conclusion découle alors directement du lemme qui suit. □

Au cours de la preuve précédente, nous venons de montrer que :

$$|x-r| < |x-s| \quad \forall s \in \mathcal{R} \setminus \{r\}. \qquad \text{(Serre proximité)}$$

En particulier, x est plus proche de r que de tous les conjugués de r sur K. On retrouve ici une notion de "proximité" qui figure par exemple dans [21], exercice 1, II, § 2 p.40. L'objet de cet exercice est de montrer le lemme :

Lemme 12 (Serre's lemma) *Soit K un corps complet pour une valeur absolue, $|\ |$, ultra-métrique. On considère x un élément algébrique séparable sur K ; on note $x_1 = x, x_2, \ldots, x_n$ ses conjugués. Si un élément y algébrique sur K vérifie :*

$$|y-x| < |y-x_i| \qquad \forall i \geqslant 2,$$

alors $x \in K(y)$.

Preuve — Soit L la $K(y)$-extension engendrée par les conjugués de x sur K ; c'est une $K(y)$-extension de degré fini, normale et séparable donc galoisienne sur $K(y)$. Montrer que $x \in K(y)$ revient donc à montrer que x est fixé par tous les $K(y)$-automorphismes de $\mathrm{Aut}_{K(y)}(L)$. Soit $\sigma \in \mathrm{Aut}_{K(y)}(L)$, il conserve la valeur absolue de L (j'entends par là l'unique prolongement à L de la valeur absolue de K), par conséquent,

$$|\sigma(y) - \sigma(x)| = |y-x| \quad \text{i.e.} \quad |y-\sigma(x)| = |y-x|.$$

Mais comme $\sigma(x)$ est un conjugué de x, par hypothèse, nécessairement $\sigma(x) = x$. □

Enfin, du lemme 12, nous pouvons déduire facilement le résultat classique de la théorie des corps locaux déjà évoqué précédemment, à savoir le lemme de Krasner :

Corollaire 12 (Krasner's lemma) *Soit K un corps complet pour une valeur absolue, $|\ |$, ultra-métrique. On considère x un élément algébrique séparable sur K ; on note $x_1 = x, x_2, \ldots, x_n$ ses conjugués. Si un élément y algébrique sur K vérifie :*

$$|y-x| < |x-x_i| \qquad \forall i \geqslant 2,$$

alors $x \in K(y)$.

Preuve — Pour $i \geqslant 2$, écrivons $y - x_i = (y-x) + (x-x_i)$; par hypothèse $|y-x| < |x-x_i|$, donc d'après P1 $|y-x_i| = |x-x_i|$. On peut donc appliquer le lemme précédent. Autrement dit, si y est proche de x au "sens de Krasner" alors y est proche de x au "sens de Serre". □

III.4 Théorème de stabilité structurelle

III.4.1 La valeur absolue du discriminant sépare les racines

Avant de s'occuper de polynômes Tschirnhaus équivalents, il est intéressant de montrer le corollaire suivant :

Corollaire 13 *Soit K un corps* ***complet*** *pour une valeur absolue ultra-métrique $|\ |$. On note A l'anneau de valuation pour K associé à $|\ |$ et on considère $F \in A[X]$* ***unitaire****. Soit $x \in A$ tel que :*

$$|F(x)| < |\operatorname{dis}(F)|,$$

alors F admet une (unique) racine r telle que :

$$|r - x| < |F'(x)|.$$

Pour établir ce corollaire, on va montrer que x vérifie les hypothèses de la proposition 8 ; pour cela, j'ai besoin du lemme suivant :

Lemme 13 *Soit K muni d'une valeur absolue* ***ultra-métrique*** *$|\ |$, A l'anneau de valuation pour K associé à $|\ |$. On considère F un polynôme de $A[X]$* ***unitaire*** *et x un élément de A. Si $|F(x)| < |\operatorname{dis}(F)|$ alors,*

$$|\operatorname{dis}(F)| \leqslant |F'(x)^2| \quad \textit{et a fortiori} \quad |F(x)| < |F'(x)^2|.$$

Preuve — Posons $\alpha = |\operatorname{dis}(F)|$. Puisque la valeur absolue $|\ |$ est ultra-métrique, l'ensemble $I = \{y \in A,\ |y| < \alpha\}$ est un idéal de A. Comme $|F(x)| < \alpha$, $x \mod I$ est donc un zéro de F dans A/I. Par suite, $F'(x)^2$ divise $\operatorname{dis}(F)$ modulo I. Autrement dit, il existe $a \in A$ et $y \in I$ tels que :

$$\operatorname{dis}(F) = aF'(x)^2 + y \quad \text{ou} \quad \operatorname{dis}(F) - y = aF'(x)^2.$$

Tenant compte du fait que $|y| < |\operatorname{dis}(F)|$, on obtient :

$$|\operatorname{dis}(F) - y| = |\operatorname{dis}(F)| = |aF'(x)^2| \leqslant |F'(x)^2|\ ;$$

ce qu'il fallait montrer. □

On est maintenant en mesure d'établir le corollaire 13 :

Preuve du corollaire 13 — On considère $x \in A$ tel que $|F(x)| < |\operatorname{dis}(F)|$. Alors d'après le lemme précédent, on a :

$$|F(x)| < |\operatorname{dis}(F)| \leqslant |F'(x)^2|.$$

Par conséquent, la proposition 8 permet directement de conclure. □

III.4.2 Le théorème de stabilité structurelle

Le théorème de stabilité structurelle donne une condition suffisante pour que deux polynômes à coefficients dans un corps, K, complet (pour une valeur absolue ultra-métrique) soient Tschirnhaus-équivalents. Tout d'abord, pour $F(X) = a_n X^n + \cdots + a_0 \in K[X]$, je pose :

$$\|F\| = \max\{|a_i|,\ 0 \leqslant i \leqslant n\}.$$

A plusieurs reprises dans la suite, nous utiliserons le fait que pour tout x entier sur l'anneau de valuation A pour K, on a :

$$|F(x)| \leqslant \|F\| \tag{P3}$$

(on note $|\ |$ l'unique prolongement de la valeur absolue $|\ |$ à toute extension algébrique de K). En effet,

$$|F(x)| \leqslant \max\{|a_i x^i|,\ 0 \leqslant i \leqslant n\} \leqslant \max\{|a_i|,\ 0 \leqslant i \leqslant n\} = \|F\|$$

car x étant entier sur A, il vérifie nécessairement $|x| \leqslant 1$. Notons aussi que pour tout polynôme $F \in K[X]$ (unitaire ou pas),

$$\|F'\| \leqslant \|F\|.$$

Nous sommes maintenant en mesure d'énoncer le résultat principal de cette section concernant les polynômes Tschirnhaus-équivalents :

Cas des polynômes unitaires à coefficients dans l'anneau de valuation

Théorème 10 *Soit K un corps* **complet** *pour une valeur absolue ultra-métrique $|\ |$. L'anneau de valuation pour K associé à $|\ |$ est toujours noté A. On considère F un polynôme unitaire de $A[X]$. Si $G \in A[X]$ unitaire vérifie :*

$$\|F - G\| < |\operatorname{dis}(F)|.$$

alors G est Tschirnhaus-équivalent à F, c'est-à-dire :

$$K[X]/\langle F\rangle \simeq K[X]/\langle G\rangle .$$

On peut d'ores et déjà remarquer que les hypothèses imposent à F et G d'être de même degré ; en effet, si ce n'était pas le cas alors on aurait $\|F-G\| = 1$ (car F et G sont supposés unitaires). Mais par hypothèse, $\|F - G\| < |\operatorname{dis}(F)|$, donc en particulier $\|F - G\| < 1$. Mieux, on va montrer, grâce au résultat suivant, que F et G ont le même discriminant en valeur absolue. Du coup l'énoncé du théorème 10 devient symétrique en F et G.

Lemme 14 *Soit K un corps muni d'une valeur absolue ultra-métrique $|\ |$. Pour tous polynômes unitaires F et G de $K[X]$, si $\|F - G\| < |\operatorname{dis}(F)|$ alors $|\operatorname{dis}(G)| = |\operatorname{dis}(F)|$.*

Preuve — On utilise une technique déjà employée plus haut. On pose $\alpha = |\operatorname{dis}(F)|$ et on s'intéresse à l'idéal I de A défini par $I = \{y \in A,\ |y| < \alpha\}$. Comme $\|F - G\| < \alpha$,

$$F \equiv G \mod I \quad \text{donc} \quad \operatorname{dis}(F) \equiv \operatorname{dis}(G) \mod I.$$

Ainsi, il existe $y \in I$ tel que :

$$\operatorname{dis}(G) = \operatorname{dis}(F) + y \quad \text{d'où} \quad |\operatorname{dis}(G)| = |\operatorname{dis}(F) + y| = |\operatorname{dis}(F)|$$

car $|y| < |\operatorname{dis}(F)|$. □

> **Remarque** – Nous proposerons ultérieurement une autre démonstration de ce résultat beaucoup plus expéditive. Elle utilise une généralisation de la propriété P2.

Passons maintenant à la preuve proprement dite du théorème 10. Nous procéderons en plusieurs étapes. Commençons par montrer que :

Lemme 15 *Pour toute racine x de F dans une K-extension, il existe une unique racine y de G appartenant à $K(x)$ telle que : $|x - y| < |G'(x)|$*

Preuve — On se place dans la K-extension $K(x)$ munie de l'unique prolongement de la valeur absolue $|\ |$. Nous allons vérifier que G et x satisfont les hypothèses du corollaire 13 ; il faut donc s'assurer que $|G(x)| < |\operatorname{dis}(G)|$. Mais,

$$|G(x)| = |G(x) - F(x)| \overset{P3}{\leqslant} \|F - G\| < |\operatorname{dis}(F)| = |\operatorname{dis}(G)| \qquad \text{par hypothèse.}$$

Ainsi (d'après le corollaire 13), G admet une unique racine $y \in K(x)$ telle que :

$$|y - x| < |G'(x)|,$$

ce qu'il fallait montrer. □

Mais comme on l'a noté précédemment, dans les hypothèses du théorème 10, les polynômes F et G jouent un rôle symétrique. Par suite, ce que l'on vient d'énoncer pour les racines de F est encore vrai pour celles de G. En particulier, à la racine y de G mise en évidence dans le lemme précédent, il correspond une unique racine $z \in K(y)$ de F cette fois telle que :

$$|z - y| < |F'(y)|.$$

Cela étant, nous allons maintenant profiter des conditions de proximité entre les racines x et z de F pour établir l'égalité $x = z$. Il nous faut pour cela vérifier que :

Lemme 16 *Avec les mêmes notations que précédemment,*

$$|F'(x)| = |F'(y)| = |G'(x)| = |G'(y)|.$$

Preuve — Commençons par montrer que $|F'(x)| = |G'(x)|$:

$$|F'(x) - G'(x)| \leqslant \|F' - G'\| \leqslant \|F - G\| < |\operatorname{dis}(F)|\ ;$$

mais comme x est une racine de F, $F'(x)^2$ divise $\operatorname{dis}(F)$, par suite, $|\operatorname{dis}(F)| \leqslant |F'(x)^2|$ donc a fortiori $|\operatorname{dis}(F)| \leqslant |F'(x)|$. En résumé, on vient de montrer que : $|F'(x) - G'(x)| < |F'(x)|$. Ainsi, en vertu de $P1$, on a bien $|F'(x)| = |G'(x)|$. Cela étant, comme $|x - y| < |G'(x)| = |F'(x)|$, la propriété P3 assure directement les deux égalités $|G'(x)| = |G'(y)|$ et $|F'(x)| = |F'(y)|$. □

Tout est désormais en place pour conclure.

Preuve du théorème 10 — Nous ne nous sommes pas encore persuadés du fait que $x = z$:

$$|x - z| = |x - y + y - z| \leqslant \max\{|x - y|, |y - z|\} < \max\{|G'(x)|, |F'(y)|\} = |F'(x)|.$$

Par conséquent, x et z étant tous deux racines de F, d'après le lemme 9, on a bien $x = z$.

En conclusion, à toute racine x de F, on a associé une racine y de G (bien précise) qui vérifie :

$$|x - y| < |G'(x)| \quad \text{et} \quad K(x) = K(y).$$

On vient donc d'exhiber deux fonctions φ et ψ :

$$\varphi\ :\ \{\text{racines de } F\} \to \{\text{racines de } G\} \quad \text{et} \quad \psi\ :\ \{\text{racines de } G\} \to \{\text{racines de } F\}$$

réciproques l'une de l'autre.

D'autre part, si x et x' sont deux racines de F, conjuguées, les racines y et y' de G qui leurs sont respectivement associées sont elles aussi conjuguées. En effet, puisque x et x' sont conjuguées, il existe $\sigma : K(x) \to K(x')$, un K-isomorphime tel que $\sigma(x) = x'$. Comme y est associée à x, on sait que $|x - y| < |G'(x)|$. Compte tenu du fait que σ préserve la valeur absolue, (à cause de l'unicité du prolongement de cette dernière), on a donc :

$$|\sigma(x) - \sigma(y)| < |G'(\sigma(x))| \quad \text{i.e.} \quad |x' - \sigma(y)| < |G'(x')|.$$

Par conséquent, $\sigma(y)$ est la racine de G associée à x', c'est à dire y'.

Chaque facteur irréductible F_1 de F est donc en correspondance avec un facteur irréductible G_1 de G. Comme de plus, si x est une des racines de F_1, la racine de G, y, qui lui correspond (que l'on sait être racine de G_1 d'après ce qui précède) vérifie $K(x) = K(y)$, on a :

$$K[X]/\left<F_1\right> \simeq K[X]/\left<G_1\right>.$$

Pour finir, si $F = F_1 \cdots F_k$ est la décomposition en irréductibles (distincts car on ne l'a pas encore remarqué mais nécessairement $|\operatorname{dis} F| = |\operatorname{dis} G| \neq 0$) de F, et $G = G_1 \cdots G_k$ celle de G, avec F_i correspondant à G_i alors :

$$K[X]/\left<F\right> \simeq K[X]/\left<F_1\right> \times \cdots \times K[X]/\left<F_k\right> \simeq K[X]/\left<G_1\right> \times \cdots \times K[X]/\left<G_k\right> \simeq K[X]/\left<G\right>$$

d'où le résultat. □

Deux autres preuves en utilisant les proximités de Serre et de Krasner

Il est aussi possible de montrer le théorème de stabilité structurelle à partir des notions de proximités au sens de Serre ou de Krasner dont il est question dans la section III.3. D'ailleurs dans [21], l'exercice 2, II, § 2 p.40 propose de montrer une forme faible du théorème de stabilité structurelle. De même, Serge Lang dans [13] propose, comme application du lemme de Krasner, un autre théorème de stabilité structurelle. Chacun des deux auteurs cités considèrent F un polynôme irréductible séparable de $K[X]$ et montrent que tout polynôme G de même degré que F et **suffisamment** proche de F est Tschirnhaus-équivalent à F. Cependant, le résultat donné au théorème 10 est un peu plus précis, dans la mesure où il avance un "epsilon", i.e. $|\operatorname{dis}(F)|$, quantifiant le "**suffisamment**". De plus, nous ne sommes pas partis d'un polynôme F irréductible au départ. En revanche, il est fondamental pour la preuve proposée que F et G soient supposés unitaires et à coefficients dans A (ce que ni Serre ni Lang ne demandent dans les deux ouvrages à peine cités) mais nous nous affranchirons de ces hypothèses par la suite. Avant cela, remontrons maintenant le théorème 10 en partant des résultats de la section III.3 :

Preuve du lemme 15 à partir de la "Serre proximité" — Je rappelle que l'on dispose de deux polynômes F et G unitaires de $A[X]$ tels que $\|F - G\| < |\operatorname{dis}(F)|$. Outre le fait que cela implique que ces deux polynômes sont de même degré, on s'est aussi convaincu de l'égalité $|\operatorname{dis}(F)| = |\operatorname{dis}(G)|$ et de la séparabilité de ces deux polynômes. Cela étant, comme précédemment, on considère x une racine de F. Alors,

$$|G(x)| = |G(x) - F(x)| \leqslant \|F - G\| < |\operatorname{dis}(F)|,$$

donc en vertu du lemme 13, G et x vérifient :

$$|G(x)| < |G'(x)|^2.$$

Ainsi, d'après la proposition 35, on sait que G admet une unique racine y telle que :

$$|x - y| < |G'(x)| \qquad \text{et} \qquad y \in K(x).$$

On vient de remontrer le lemme 15. Pour conclure, comme précédemment, on utilise la symétrie des hypothèses. $\square$

Preuve du lemme 15 à partir de la "Krasner proximité" — Un nouvelle fois, on considère x une racine de F. Notons $y_1, y_2, \ldots, y_n$ les racines (distinctes) de G ; quitte à renuméroter les y_i, on suppose que y_1 vérifie $|x - y_1| = \min\{|x - y_i|,\ i \geqslant 1\}$. De la même manière que précédemment, on a $|G(x)| < |\operatorname{dis}(G)|$, ou encore :

$$\prod_{i=1}^{n} |x - y_i| < |G'(y_1)| \cdots |G'(y_n)|.$$

Remarquons maintenant que pour $i \neq j$, nécessairement,

$$|y_i - y_j| \geqslant |G'(y_i)| \ ;$$

en effet, sinon d'après le lemme 9, on aurait $y_i = y_j$. Ainsi,

$$\begin{aligned}\prod_{i=1}^{n} |x - y_i| &< |G'(y_1)|\ |y_2 - y_1| \cdots |y_n - y_1| \\ &\leqslant |G'(y_1)|\ \max\{|y_2 - x|, |x - y_1|\} \cdots \max\{|y_n - x|, |x - y_1|\} \\ &\leqslant |G'(y_1)|\ |y_2 - x| \cdots |y_n - x| \qquad \text{de par le choix de } y_1.\end{aligned}$$

En simplifiant, on obtient :

$$|x - y_1| < |G'(y_1)| \ ;$$

et comme pour tout $i \geqslant 2$, $|G'(y_1)| \leqslant |y_i - y_1|$, on vient donc de montrer que x est proche de y_1 au sens de Krasner. Par conséquent, d'après le lemme qui porte le nom de ce dernier (lemme 12), $y_1 \in K(x)$ et on peut de nouveau conclure grâce à la symétrie des hypothèses. $\square$

Passage aux polynômes quelconques

Afin d'obtenir un résultat concernant les polynômes à coefficients dans K, j'introduis pour un polynôme $F(X) = aX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$, de degré n (non nécessairement unitaire), l'unitarisé de F, noté F_{u} et défini par :

$$F_{\mathrm{u}}(X) = a^{n-1}F(X/a) = X^n + a_{n-1}aX^{n-1} + \cdots + a_0a^n \ ;$$

c'est un polynôme unitaire à coefficients entiers. Bien sûr, les polynômes F et F_{u} sont Tschirnhaus-équivalents et leurs discriminants sont égaux au carré d'un inversible près. Commençons par montrer que :

Proposition 36 *Soit K un corps* ***complet*** *pour une valeur absolue ultra-métrique $|\ |$. L'anneau de valuation pour K associé à $|\ |$ est toujours noté A. On considère un polynôme $F \in A[X]$ de degré n. Si $G \in K[X]$ de degré n vérifie :*

$$\|F - G\| < |\operatorname{dis}(F_u)|.$$

alors G est Tschirnhaus-équivalent à F.

Remarque – Comme dans le cas unitaire, de l'hypothèse $\|F - G\| < |\operatorname{dis}(F_{\mathrm{u}})|$, il résulte en particulier que $\operatorname{dis}(F_{\mathrm{u}}) \neq 0$; par suite les polynômes F et F_{u} sont nécessairement séparables.

Au cours de la preuve qui suit, nous allons utiliser une propriété qui ne sera démontrée qu'ultérieurement ; il s'agit de la propriété P2' de la section IV.2. Nous avons tous les moyens pour l'établir dès maintenant, mais sa place se justifie plus dans la section citée plus haut.

Preuve — Nous allons bien sûr nous ramener au théorème 10 en établissant que :

$$\|F_{\mathrm{u}} - G_{\mathrm{u}}\| < |\operatorname{dis}(F_{\mathrm{u}})|$$

dès lors, F_{u} et G_{u} sont Tschirnhaus-équivalents. Il en est donc de même de F et G.

Comme dans le cas des constantes, de l'inégalité,

$$\|F - G\| < |\operatorname{dis}(F_{\mathrm{u}})| \leqslant 1,$$

on déduit que G est nécessairement à coefficients entiers. Ecrivons maintenant :

$$F(X) = aX^n + a_{n-1}X^{n-1} + \cdots + a_0 \qquad \text{et} \qquad G(X) = bX^n + b_{n-1}X^{n-1} + \cdots + b_0,$$

alors appliquant la propriété P2' au polynôme $X^{n-i}Y$, il vient :

$$\forall\, 0 \leqslant i \leqslant n, \quad |a^{n-i}a_i - b^{n-i}b_i| \leqslant \max\{|a-b|, |a_i - b_i|\}$$

de sorte que $\|F_{\mathrm{u}} - G_{\mathrm{u}}\| \leqslant \|F - G\| < |\operatorname{dis}(F_{\mathrm{u}})|$, ce que l'on voulait. □

Plus rien ne nous empêche, désormais, de considérer des polynômes quelconques ; montrons que :

Corollaire 14 *Pour tout polynôme séparable $F \in K[X]$ de degré n, on peut expliciter $\varepsilon_F > 0$, tel que pour tout $G \in K[X]$* ***de degré*** *n, dès que $\|F - G\| < \varepsilon_F$, F et G sont Tschirnhaus-équivalents.*

Preuve — Il suffit de considérer $d \in A \setminus \{0\}$ tel que $dF \in A[X]$ (un des dénominateurs des coefficients de F convient puisque A est un anneau de valuation) ; alors, posant $\varepsilon_F = |\operatorname{dis}((dF)_{\mathrm{u}})|/|d|$, l'inégalité $\|F - G\| < \varepsilon_F$ implique $\|dF - dG\| < |\operatorname{dis}(dF)_{\mathrm{u}}|$ et on est ramené au cas précédent. □

III.4.3 Applications et contre-exemple

Dans cette section, nous donnons une application du théorème de stabilité structurelle ainsi, qu'un contre-exemple qui figure dans les exercices de [3].

• Classiquement, on montre grâce au théorème de stabilité structurelle que le nombre d'extensions d'un corps local localement compact K (i.e. à corps résiduel fini) de degré fixé est fini. J'en rappelle rapidement la preuve qui figure par exemple dans [13], Chap II, §5, Proposition 14. Il suffit d'établir qu'il n'existe qu'un nombre fini d'extensions de K totalement ramifiées de degré donné. En effet, toute extension de K se décompose en une tour d'extensions, la première étant non ramifiée et la seconde totalement ramifiée, et on connaît déjà l'unicité des extensions non ramifiées de degré fixé. Notons A l'anneau de valuation de K et π une uniformisante de K. L'anneau A est compact, compte tenu de la locale compacité. Soit $\mathcal{E}(n)$ l'ensemble des polynômes d'Eisenstein (pour π) de degré n à coefficients dans l'anneau A. Alors,

$$\mathcal{E}(n) = \{1\} \times \pi A \times \cdots \times \pi A \times \pi\mathcal{U}(A).$$

A étant compact, $\mathcal{U}(A)$ l'est aussi (car fermé dans A), donc $\mathcal{E}(n)$ est lui encore un compact. Maintenant, pour $F \in \mathcal{E}(n)$, je pose :

$$V_F = \{1\} \times \mathcal{B}(F, |\operatorname{dis}(F)|) \times \cdots \times \mathcal{B}(F, |\operatorname{dis}(F)|) \;\cap\; \mathcal{E}(n) \;;$$

c'est un ouvert de $\mathcal{E}(n)$. Bien sûr, les ouverts V_F pour $F \in \mathcal{E}(n)$ forment un recouvrement d'ouverts de $\mathcal{E}(n)$. Ainsi, l'ensemble $\mathcal{E}(n)$ étant compact, il est recouvert par un nombre fini de V_F.

Mais pour tout $G \in V_F$, d'après le théorème 10, F et G sont Tschirnhaus-équivalents. Par conséquent, nous venons de montrer qu'il n'existe qu'un nombre fini de classes d'isomorphie de polynômes d'Eisenstein. Les extensions totalement ramifiées étant toutes définies par de tels polynômes, on conclut aisément.

• Dans un corps cubique de nombres, K, le premier 2 peut être diviseur essentiel. Je rappelle que cela signifie que 2 divise tous les indices $[\mathcal{O} : A]$, où $\mathcal{O}$ est l'anneau des entiers de K et A un quelconque ordre monogène de K, c'est à dire un sous-anneau de K de la forme $\mathbb{Z}[\theta]$ avec θ un élément primitif de K sur $\mathbb{Z}$.

Remarques

1. En particulier, si 2 est diviseur essentiel d'un corps cubique alors l'anneau des entiers de ce corps ne peut pas être monogène.

2. Plus généralement, si K est un corps de nombres de degré n, alors ses éventuels diviseurs essentiels sont nécessairement inférieurs (strictement) à n (c.f. [17], Chap 4, §3, n°2, Proposition 4.17).

En fait, les corps cubiques pour lesquels 2 est diviseur essentiel sont ceux dans lequels l'idéal engendré par 2 se décompose totalement ; cela est dû au fait qu'il n'existe que deux polynômes irréductibles linéaires sur $\mathbb{F}_2$ (c.f. le corollaire de la proposition de [17] référée précédemment). Nous allons utiliser cette caractérisation pour construire des polynômes cubiques à coefficients entiers dont une quelconque racine engendre un corps cubique qui admet 2 comme diviseur essentiel. On définit, pour tout triplet $t = (\alpha, \beta, \gamma)$, avec α, β, γ trois éléments de $\mathbb{Z}_2$ **distincts deux à deux**, le polynôme :

$$P_t(X) = (X - \alpha)(X - \beta)(X - \gamma)$$

Alors, conservant les notations précédentes, la boule $\mathcal{B}(P_t, |\operatorname{dis}(P_t)|_2)$ est constituée de polynômes de $\mathbb{Z}_2[X]$ tous Tschirnhaus-équivalents à P_t. En particulier, ces polynômes sont tous séparables et totalement scindés dans $\mathbb{Z}_2[X]$. Par suite, si $\operatorname{Irr}(\mathbb{Z}[X])$ désigne l'ensemble des polynômes irréductibles de $\mathbb{Z}[X]$, alors tous les polynômes de l'intersection :

$$\mathcal{B}(P_t, |\operatorname{dis}(P_t)|_2) \cap \operatorname{Irr}(\mathbb{Z}[X])$$

engendrent un corps cubique admettant 2 pour diviseur essentiel ; en effet on sait qu'il y a une correspondance bijective entre les facteurs irréductibles d'un polynôme $F \in \mathbb{Z}[X]$ dans $\mathbb{Z}_2[X]$ et les idéaux premiers au dessus de 2, du corps de nombres engendré par une quelconque des ses racines.

Par exemple, pour $t = (0, 1, -1)$, $\operatorname{dis}(P_t) = 4$, ce qui montre que les polynômes de la forme :

$$X^3 + 8aX^2 + (8b - 1)X + 8c \qquad \text{avec} \quad a, b, c \in \mathbb{Z}$$

s'ils sont de surcroît irréductibles sur $\mathbb{Q}$, conviennent. Notons que le triplet $t = (1, 2, 4)$, met en avant les polynômes de la forme :

$$X^3 + (-7 + 8a)X^2 + (14 + 8b)X - 8 + 8c \qquad \text{avec} \quad a, b, c \in \mathbb{Z}$$

Pour $a = 1$, $b = -2$ et $c = 2$, on retrouve le fameux polynôme dû à Dedekind, à savoir $X^3 + X^2 - 2X + 8$.

• Dans le corollaire 14, le polynôme considéré est supposé séparable. Cette hypothèse est fondamentale comme l'illustre l'exemple suivant. On se place dans le corps $\mathbb{F}_p((T))$ que l'on munit évidemment de la valuation associée au premier T. Posons, dans $\mathbb{F}_p((T))[X]$:

$$F(X) = X^p - T \qquad \text{et} \qquad F_n(X) = X^p + T^n X - T, \quad \forall n \geqslant 1$$

Ces polynômes sont tous irréductibles sur $\mathbb{F}_p((T))$ (ce sont des polynômes d'Eisentein) ; les F_n sont séparables alors que F ne l'est pas. De plus :

$$\lim_{n \to +\infty} \|F - F_n\| = \lim_{n \to +\infty} |T^n| = 0$$

Les polynômes F_n peuvent donc être arbitrairement proches de F ; pourtant aucun des F_n n'est Tschirnhaus-équivalent à F puisque l'un de ces polynômes est séparable alors que l'autre ne l'est pas. L'hypothèse de séparabilité du corollaire 14 est donc loin d'être superflue.

En adjoignant à $\mathbb{F}_p((T))$ toutes les racines des polynômes F_n, on obtient une extension algébrique séparable de $\mathbb{F}_p((T))$, que l'on note K ; la valeur absolue de $\mathbb{F}_p((T))$ se prolonge à K (de manière unique). Tous les polynômes F_n sont séparables et scindés dans K. Le polynôme F, lui, est encore irréductible sur K (car $\sqrt[p]{T} \notin K$; sinon cet élément serait séparable sur $\mathbb{F}_p((T))$). Nous venons donc de construire un polynôme F à coefficients dans un corps K, irréductible, non séparable et qui peut être approché de façon arbitrairement proche par des polynômes réductibles (même totalement scindés). Ceci est l'objet de la question d) de l'exercice §8 n°12 de [3].

IV Le lemme de Hensel

IV.1 A propos de norme sup

Comme toujours, on se place sur un corps K muni d'une valeur absolue $|\ |$ ultra-métrique ; A désigne l'anneau de valuation pour K associé à la valeur absolue $|\ |$. Soit M un A-module libre de dimension finie. Une base $\mathcal{B}$ de M sur A étant fixée, on peut munir M de la norme sup usuelle que l'on note $\|\ \|$. Bien sûr $\|\ \|$ vérifie encore :

$$\|x\| \leqslant 1,\ \forall x \in M, \quad \|\lambda x\| = |\lambda| \|x\|\ \forall x \in M,\ \lambda \in A \quad \text{et} \quad \|x + y\| \leqslant \max\{\|x\|, \|y\|\}\ \forall x, y \in M.$$

Tout d'abord, on remarque que cette norme est indépendante de la base choise ; en effet, soit $\mathcal{B}'$ une autre base de M sur A et $\| \ \|'$ la norme sup sur M qui lui est associée. Alors pour $x = \sum \lambda_i e_i \in M$ où les vecteurs $(e_i)_{1 \leqslant i \leqslant n}$ forment la base $\mathcal{B}$, on a :

$$\|x\|' = \left\| \sum \lambda_i e_i \right\|' \leqslant \max\{\|\lambda_i e_i\|'\} = \max\{|\lambda_i| \|e_i\|'\} \leqslant \max\{|\lambda_i|\} = \|x\| \quad \text{car} \quad \|e_i\|' \leqslant 1 \ \forall i.$$

Par symétrie on a bien évidemment $\|x\| \leqslant \|x\|'$ d'où l'égalité entre les deux normes. Dans le même ordre d'idée, pour toute $u \in \mathcal{L}(M)$ application A-linéaire de M vers M, on a :

$$\forall x \in M, \qquad \|u(x)\| \leqslant \|x\| \ ;$$

en effet,

$$\|u(x)\| = \|u(\lambda_1 e_1 + \cdots + \lambda_n e_n)\| \leqslant \max\{\|\lambda_i u(e_i)\|\} \leqslant \max\{|\lambda_i|\} = \|x\|.$$

De même, pour toute $v \in \mathcal{L}^2(M)$ application bilinéaire de $M \times M$ vers M, on a :

$$\forall x, y \in M, \qquad \|v(x, y)\| \leqslant \|x\| \|y\| \ ;$$

IV.2 Une méthode Newton à "plusieurs variables"

Soit $F : M \to M$ une application polynomiale i.e. chaque application coordonnée est un polynôme en les coordonnées. Comme nous l'avons déja fait dans le cas d'une variable, nous pouvons considérer un zéro approché de F : soit $x \in M$ tel que :

$$\|F(x)\| < |\det(DF(x))|^2. \tag{$**$}$$

Nécessairement $\det(DF(x)) \neq 0$. A ce stade, dans le cas d'une variable, on introduisait l'itéré de Newton de x. Ce dernier n'est rien d'autre que x auquel on a retranché un terme correctif de la forme $F(x)/F'(x)$. Ce terme correctif vérifie entre autres :

$$F'(x) \frac{F(x)}{F'(x)} = F(x).$$

Autrement dit, c'est un antécédent de $F(x)$ par l'application linéaire $F'(x)$. De la même façon ici, nous allons construire un itéré de Newton en retranchant à x un antécédant h_x de $F(x)$ par l'application linéaire $DF(x)$, à savoir :

$$h_x = \frac{\widetilde{DF(x)}.F(x)}{\det(DF(x))}.$$

Remarquons que $h_x \in M$ car :

$$\begin{aligned} \|h_x\| &= \|\widetilde{DF(x)}.F(x)\| / |\det(DF(x))| \\ &\leqslant \|F(x)\| / |\det(DF(x))| \qquad \text{car } \widetilde{DF(x)} \text{ est linéaire} \\ &< 1 \qquad \text{par hypothèse.} \end{aligned}$$

L'itéré de Newton y élément de M est donc défini par :

$$y = x - h_x$$

Le lemme 8, qui au début de cette section, nous a permis d'élaborer un procédé itératif a lui aussi un analogue ici ; il faut tout d'abord introduire pour $z \in M$ tel que $\det(DF(z)) \neq 0$ la quantité :

$$\rho_z = \frac{\|F(z)\|}{|\det(DF(z))|^2}.$$

Lemme 17 *On conserve les notations précédentes. Soit $x \in M$ tel que :*

$$\|F(x)\| < |\det(DF(x))|^2 \ ; \tag{$**$}$$

si y est défini par :

$$y = x - h_x,$$

alors y vérifie :

$$|\det(DF(x))| = |\det(DF(y))| \qquad \textit{et} \qquad \rho_y \leqslant \rho_x^2.$$

Avant de passer à la preuve de ce résultat, il nous faut démontrer une version “à plusieurs variables” de la propriété P2.

Lemme 18 *Soit P un polynôme de $A[X_1, \ldots, X_n]$. Si $x_1, \ldots, x_n, y_1, \ldots, y_n$ sont entiers sur A alors :*

$$|P(x_1, \ldots, x_n) - P(y_1, \ldots, y_n)| \leqslant \max\{|x_i - y_i|\}. \tag{P2'}$$

Preuve — Pour $n = 1$, cette propriété n'est rien d'autre que la propriété P2. On procède par récurrence. On écrit :

$$\begin{aligned}
&|P(x_1, \ldots, x_n) - P(y_1, \ldots, y_n)| \\
&\qquad = |P(x_1, \ldots, x_n) - P(x_1, \ldots, x_{n-1}, y_n) + P(x_1, \ldots, x_{n-1}, y_n) - P(y_1, \ldots, y_n)| \\
&\qquad \leqslant \max\{|P(x_1, \ldots, x_n) - P(x_1, \ldots, x_{n-1}, y_n)|, |P(x_1, \ldots, x_{n-1}, y_n) - P(y_1, \ldots, y_n)|\} \\
&\qquad \leqslant \max\{|x_n - y_n|, \max_{1 \leqslant i \leqslant n-1}\{|x_i - y_i|\}\} = \max_{1 \leqslant i \leqslant n}\{|x_i - y_i|\},
\end{aligned}$$

en utilisant l'hypothèse de récurrence et P2. □

Remarque – Grâce à ce résultat, nous pouvons proposer une deuxième preuve du lemme 14. Je rappelle qu'il s'agissait de montrer que si $\|F - G\| < |\operatorname{dis}(F)|$ alors $|\operatorname{dis}(F)| = |\operatorname{dis}(G)|$. Mais comme $\operatorname{dis}(F)$ est un polynôme en les coefficients de F, on montre directement, en appliquant le résultat précédent, que :

$$|\operatorname{dis}(F) - \operatorname{dis}(G)| \leqslant \|F - G\|,$$

d'où le résultat.

Nous sommes maintenant en mesure de donner la preuve de la généralisation du lemme 8 :

Preuve du lemme 17 — On remarque, tout d'abord, que l'application $x \longmapsto \det(DF(x))$ étant polynomiale (en les coordonnées de x), d'après P2',

$$|\det(DF(x)) - \det(DF(y))| \leqslant \|x - y\|.$$

De plus,

$$\begin{aligned}
\|y - x\| = \|h_x\| &= \left\| \frac{\widetilde{DF(x)}.F(x)}{\det(DF(x))} \right\| \\
&\leqslant \frac{\|F(x)\|}{|\det(DF(x))|} \qquad \text{car } \widetilde{DF(x)} \text{ est une application } A\text{-linéaire} \\
&< |\det(DF(x))| \qquad \text{car on a supposé } \|F(x)\| < |\det(DF(x))|.
\end{aligned}$$

Par conséquent, $|\det(DF(x)) - \det(DF(y))| < |\det(DF(x))|$, et l'éternelle propriété P1 aidant, on montre que :

$$|\det(DF(x))| = |\det(DF(y))|.$$

Il reste à établir la deuxième inégalité. Pour ce faire, on utilise de nouveau une formule de Taylor à l'ordre 2 : $F(X + H) - F(X) - DF(X).H = \Delta F(X, H).(H, H)$, où $\Delta F(X, H)$ est une application bilinéaire telle que $\Delta F(X, X) = DF(X)$. Appliqué à y, cela donne :

$$F(y) = F(x) - DF(x).h_x + \Delta F(x, h_x).(h_x, h_x) = \Delta F(x, h_x).(h_x, h_x)$$

d'où :

$$\|F(y)\| \leqslant \|h_x\|^2$$

car $D(x, h_x)$ est une application bilinéaire. Pour conclure, il suffit de revenir à la définition de ρ_y :

$$\rho_y = \frac{\|F(y)\|}{|\det(DF(y))|^2} \leqslant \frac{\|h_x\|^2}{|\det(DF(x))|^2} \leqslant \rho_x^2$$

ce qu'il fallait établir. □

Cela étant, on peut désormais déduire du lemme précédent le pendant "à plusieurs variables" du corollaire 8 donnant une condition pour qu'une fonction polynomiale $F : M \to M$ admette une racine dans M. Cependant, il convient de montrer tout d'abord un lemme qui assurera des conditions d'unicité dans la suite :

Lemme 19 *Soit K un corps muni d'une valeur absolue ultra-métrique $|\ |$; on note A l'anneau de valuation pour K associé à $|\ |$. On considère M un A-module libre de rang fini et $F : M \to M$ une fonction polynomiale. Pour tous x, y éléments de M tels que $F(x) = F(y)$, si $\|x - y\| < |\det(DF(x))|$ alors $x = y$.*

Preuve — Ecrivons $F(x) - F(y) = \Delta F(x, y).(x - y)$ où $\Delta F(x, y) : M \to M$ est une application linéaire et $\Delta F(x, x) = DF(x)$. Nous allons montrer que $\Delta F(x, y)$ est injective ce qui assurera bien que $x = y$. Pour cela, il suffit de s'assurer que $\det(\Delta F(x, y)) \neq 0$. On introduit I l'idéal de A défini par $I = \{a \in A,\ |a| < |\det(DF(x))|\}$, puis le sous A-module de M, $N = IM$. On vérifie facilement que $N = \{b \in M,\ \|b\| < |\det(DF(x))|\}$. Alors l'hypothèse $\|x - y\| < |\det(DF(x))|$ se traduit par $x \equiv y \mod N$ et donc modulo I :

$$\det(\Delta F(\overline{x}, \overline{y})) = \det(\Delta F(\overline{x}, \overline{x})) = \det(DF(\overline{x})).$$

Mais par définition de I, $\det(DF(x)) \notin I$, i.e. $\det(DF(\overline{x})) \neq 0$. Par suite, $\det(\Delta F(\overline{x}, \overline{y})) \neq 0$ donc a fortiori $\det(\Delta F(x, y)) \neq 0$. □

Nous sommes désormais en mesure d'énoncer le résultat principal de cette section :

Corollaire 15 *Soit K un corps* ***complet*** *pour une valeur absolue ultra-métrique $|\ |$; on note A l'anneau de valuation pour K associé à $|\ |$. On considère M un A-module libre de rang fini et $F : M \to M$ une fonction polynomiale. Soit $x \in M$ tel que :*

$$\|F(x)\| < |\det(DF(x))|^2 \qquad (**)$$

alors la suite $(x_k)_k$ de M définie par :

$$x_0 = x \qquad et \qquad x_{k+1} = x_k - \frac{\widetilde{DF(x_k)}.F(x_k)}{\det(DF(x_k))} \quad \forall k \geqslant 0,$$

converge vers une racine r de F dans M. De plus, r est l'unique racine telle que :

$$\|r - x\| < |\det(DF(x))|.$$

Preuve — La preuve de l'existence consiste à tirer profit du lemme 17 pour réitérer la construction de Newton. On procède comme dans la preuve du corollaire 8 ; on utilise le fait que :

$$|\det(DF(x_k))| = |\det(DF(x_{k-1}))| = |\det(DF(x_0))| \qquad \text{et} \qquad \rho_k \leqslant \rho_{k-1}^2 \leqslant \rho_0^{2^k} \quad \text{où : } \rho_k = \rho_{x_k}.$$

Quant à l'unicité, elle découle directement du lemme 19. □

IV.3 Le lemme de Hensel, enfin !

Nous allons maintenant déduire de tout ce qui précède le lemme de Hensel. Plutôt que d'énoncer directement ce résultat sous sa forme la plus classique (j'entends par là la version qui a la faveur de la plupart des auteurs), je préfère, dans un premier temps, donner un théorème sensiblement plus général. Ce dernier figure dans [2], théorème 1 p 304 ; néanmoins la preuve proposée ici en est différente.

Théorème 11 *Soit K un corps* ***complet*** *pour une valeur absolue ultra-métrique $|\ |$; on note A l'anneau de valuation pour K associé à $|\ |$. Soit F, G_0 et H_0 trois polynômes de $A[X]$ tels que F et G_0H_0 aient* ***même degré*** *et* ***même coefficient dominant****. Si*

$$\|F - G_0H_0\| < |\operatorname{res}(G_0, H_0)|^2$$

alors il existe G et H deux polynômes de $A[X]$ uniques, de ***même degré*** *et de* ***même coefficient dominant*** *que G_0 et H_0 respectivement, tels que :*

$$F = GH, \quad \|G - G_0\| < |\operatorname{res}(G_0, H_0)| \quad et \quad \|H - H_0\| < |\operatorname{res}(G_0, H_0)|.$$

Preuve — L'idée de la preuve est bien sûr d'utiliser le corollaire 15. Pour cela, pour $d > 0$, on note $A_d[X] = \{P \in A[X],\ \deg P < d\}$ et on considère l'application :

$$\begin{array}{rccc} \varphi: & A_m[X] \times A_n[X] & \longrightarrow & A_{m+n}[X] \\ & (P,Q) & \longmapsto & (aX^m + P)(bX^n + Q) - F \end{array}$$

où $(m,n) \in \mathbb{N}^2$ et $(a,b) \in A^2$ sont les degrés et coefficients dominants respectifs de G_0 et H_0. Considérons φ comme une application du A-module libre A^{m+n} dans lui-même ; φ est alors une fonction polynomiale dont on connaît un zéro approché : le couple (P_0, Q_0) où P_0 et Q_0 sont les deux polynômes tels que :

$$G_0 = aX^m + P_0 \qquad \text{et} \qquad H_0 = bX^n + Q_0.$$

En effet, la différentielle de φ au point (P_0, Q_0), c'est l'application linéaire :

$$(U,V) \longmapsto (aX^m + P_0)V + (bX^n + Q_0)U = G_0V + H_0U,$$

dont le déterminant n'est rien d'autre que $\operatorname{res}(G_0, H_0)$. En conséquence, on a par hypothèse sur G_0 et H_0 :

$$\|\varphi(P_0,Q_0)\| < |\det(D\varphi(P_0,Q_0))|^2 = |\operatorname{res}(G_0,H_0)|^2,$$

et (P_0, Q_0) est bien un zéro approché de φ. On peut appliquer le corollaire 15 : il existe donc un zéro de φ $(P,Q) \in A_n[X] \times A_m[X]$ qui vérifie :

$$\|P - P_0\| < |\operatorname{res}(G_0,H_0)| \quad \text{et} \quad \|Q - Q_0\| < |\operatorname{res}(G_0,H_0)|.$$

Autrement dit, si on pose $G = aX^m + P$ et $H = bX^n + Q$, ces deux polynômes vérifient :

$$F = GH, \quad \|G - G_0\| < |\operatorname{res}(G_0,H_0)| \quad \text{et} \quad \|H - H_0\| < |\operatorname{res}(G_0,H_0)|$$

ce que l'on voulait. □

Avant de passer au lemme de Hensel sous sa forme la plus connue (c'est un cas particulier du théorème 11), nous allons fixer quelques notations. Si A est un anneau local, nous noterons $\mathfrak{m}$ son idéal maximal et $k = A/\mathfrak{m}$ le corps résiduel. Tous les polynômes de $A[X]$ seront désignés par une lettre majuscule, tous ceux de $k[X]$ par une lettre minuscule. De plus, pour F un polynôme de $A[X]$, la réduction de F modulo $\mathfrak{m}$ sera toujours notée $\overline{F}$; le polynôme $\overline{F}$ est donc élément de $k[X]$. Cela étant, montrons tout d'abord que :

Lemme 20 *Soit A un anneau local dont on note $\mathfrak{m}$ l'idéal maximal et $k = A/\mathfrak{m}$ le corps résiduel. On considère $F \in A[X]$ non nul modulo $\mathfrak{m}$ et g,h deux polynômes de $k[X]$ tels que $\overline{F} = gh$. On peut choisir G et H dans $A[X]$ deux représentants de g et h respectivement tels que :*

$$\deg G = \deg g, \quad \deg GH = \deg F \quad \textit{et} \quad \operatorname{lc}(GH) = \operatorname{lc}(F).$$

De plus, si g est unitaire, alors G peut être choisi unitaire.

Preuve — On commence par choisir $G \in A[X]$ un représentant de g de degré $\deg(g)$. Alors nécessairement $\operatorname{lc}(G) \notin \mathfrak{m}$, donc $\operatorname{lc}(G)$ est inversible dans A. Il nous reste à choisir H un représentant de h. On veut que ce dernier vérifie :

$$\deg H = \deg F - \deg G = \deg F - \deg g \qquad \text{et} \qquad \operatorname{lc}(H) = \operatorname{lc}(F)/\operatorname{lc}(G).$$

Autrement dit, nous avons ramené le problème à la question : étant donné $h \in k[X]$, est-il possible de choisir $H \in A[X]$ un représentant de h de degré d donné ($d = \deg(F) - \deg(g)$) et de coefficient dominant, a donné ($a = \operatorname{lc}(F)/\operatorname{lc}(G)$) ?

La réponse à la question est positive si et seulement si $d \geqslant \deg(h)$ et si $\overline{a} = \operatorname{coeff}_d(h)$.

Dans notre cadre, on a toujours $d \geqslant \deg(h)$ car $\deg(F) \geqslant \deg(\overline{F}) = \deg(g) + \deg(h)$. Pour vérifier la deuxième condition, on distingue deux cas :

- Si $\deg(F) = \deg(\overline{F})$, i.e. $\operatorname{lc}(F)$ inversible modulo $\mathfrak{m}$, alors $d = \deg(h)$ et $\overline{\operatorname{lc}(G)}\operatorname{lc}(h) = \overline{\operatorname{lc}(F)}$, i.e. $\overline{a} = \operatorname{lc}(h) = \operatorname{coeff}_d(h)$.
- Sinon, c'est à dire si $\operatorname{lc}(F) \in \mathfrak{m}$ alors $d > \deg(h)$ et $\overline{a} = 0 = \operatorname{coeff}_d(h)$. □

Remarque – Le fait que l'anneau A soit local est primordial ici. Par exemple, sur $\mathbb{Z}$, le lemme précédent peut être mis en défaut : soit $F = 19X^2 + 5X + 1$ et $p = 13$ alors,

$$F \equiv 6X^2 + 5X + 1 \equiv (2X+1)(3X+1) \mod 13.$$

Comme 19 est premier, on ne peut pas espérer trouver deux polynômes G et H comme dans le lemme 20. La condition $\mathrm{lc}(GH) = \mathrm{lc}(F)$ est bien trop contraignante !

Lemme 21 (de Hensel) *Soit K un corps **complet** pour une valeur absolue ultra-métrique $|\ |$; on note A l'anneau de valuation pour K associé à $|\ |$, $\mathfrak{m}$ l'idéal maximal de A et $k = A/\mathfrak{m}$ le corps résiduel. Soit F un polynôme de $A[X]$. Si g et h sont deux polynômes premiers entre eux de $k[X]$, tels que :*

$$\overline{F} = gh,$$

alors il existe deux polynômes G et H de $A[X]$ uniques, tels que :

$$F = GH, \quad \overline{G} = g, \quad \overline{H} = h \quad \text{et} \quad \deg G = \deg g.$$

De plus, si g est unitaire, alors G peut être choisi unitaire.

Preuve — Rappelons tout d'abord que A étant un anneau de valuation, il est local. Nous pouvons donc appliquer le lemme 20. Ce dernier nous assure l'existence de deux représentants respectifs de g et h, G_0 et H_0 de $A[X]$ tels que :

$$\deg G_0 = \deg g, \quad \deg G_0H_0 = \deg F \quad \text{et} \quad \mathrm{lc}(G_0H_0) = \mathrm{lc}(F).$$

De plus, $F \equiv G_0H_0 \mod \mathfrak{m}$, autrement dit,

$$\|F - G_0H_0\| < 1.$$

Enfin, le polynôme G_0 ne chutant pas de degré modulo $\mathfrak{m}$ (ce qui est équivalent au fait que $\mathrm{lc}(G_0)$ est inversible modulo $\mathfrak{m}$) et g et h étant supposés premiers entre eux, on a :

$$\overline{\mathrm{res}(G_0, H_0)} \sim \mathrm{res}(\overline{G}_0, \overline{H}_0) = \mathrm{res}(g, h) \not\equiv 0 \mod \mathfrak{m}\ ;$$

en conséquence, $\mathrm{res}(G_0, H_0)$ est inversible modulo $\mathfrak{m}$, i.e. $|\,\mathrm{res}(G_0, H_0)| = 1$. Par suite, le lemme de Hensel est un cas particulier du théorème 11. □

IV.4 Applications

Commençons par donner un corollaire du théorème 11 ; dans le cadre de la méthode de Newton, nous avons déjà montré ce type de résultat, il s'agissait du corollaire 13.

Proposition 37 *Soit K un corps **complet** pour une valeur absolue ultra-métrique $|\ |$; on note A l'anneau de valuation associé à $|\ |$. Soit F un polynôme unitaire de $A[X]$. Si G_0 et H_0 sont deux polynômes unitaires de $A[X]$ tels que :*

$$\|F - G_0H_0\| < |\,\mathrm{dis}(F)|$$

alors F se factorise dans $A[X]$. Plus précisément, il existe G et H deux polynômes de $A[X]$ tels que :

$$F = GH \qquad \text{avec} \qquad \|G - G_0\| < |\,\mathrm{res}(G_0, H_0)| \quad \text{et} \quad \|H - H_0\| < |\,\mathrm{res}(G_0, H_0)|.$$

Preuve — Puisque $\|F - G_0H_0\| < |\,\mathrm{dis}(F)|$, on sait grâce au lemme 14 que $|\,\mathrm{dis}(F)| = |\,\mathrm{dis}(G_0H_0)|$. Mais il est bien connu que $\mathrm{dis}(G_0H_0) = \mathrm{dis}(G_0)\,\mathrm{dis}(H_0)\,\mathrm{res}(G_0, H_0)^2$, ainsi :

$$|\,\mathrm{dis}(F)| = |\,\mathrm{dis}(G_0)\,\mathrm{dis}(H_0)\,\mathrm{res}(G_0, H_0)^2| \leqslant |\,\mathrm{res}(G_0, H_0)^2|$$

et par suite $\|F - G_0H_0\| < |\,\mathrm{res}(G_0, H_0)^2|$. Autrement dit, F, G_0 et H_0 vérifient les hypothèses du théorème 11 ; ce dernier permet directement de conclure. □

Annexe :

Il est difficile (et peut être même dénué d'intérêt) de lire un ouvrage de mathématiques comme on lit généralement un roman à savoir en commençant par la première ligne et en terminant par la dernière[13]. Il est généralement salutaire (pour la compréhension) de faire des sauts dans la lecture. Cela permet de raccrocher un passage à son bagage mathématique personnel et de comprendre ainsi où nous mène l'auteur. Pour avoir tenté de lire le chapitre 6 d'algèbre commutative de Bourbaki ([3]) de manière linéaire, je me suis vite aperçu que j'allais dans le mur. Je venais de comprendre la théorie des anneaux de Dedekind, et il se trouve que la lecture de la Proposition 6 du chapitre 6, §8, n°6 de [3] (qui figure presqu'à la fin du chapitre) me permettait de réinvestir ce que je venais d'apprendre. Cette section peut être vue comme le petit journal de bord que j'ai écrit ou cours de la lecture (étalée sur une longue période et entrecoupée de beaucoup de lectures sur le sujet et sur d'autres) de ce fameux chapitre du maître Bourbaki, qui reste, concernant la théorie des valuations, l'une des références incontestables. En aucun cas, il ne s'agit ici de rivaliser avec ce classique ni même avec les autres d'ailleurs...

A Prolongement de valuations revisité

A.1 Introduction aux anneaux de valuation

Certains résultats de cette section figurent déjà au tout début de ce papier. Je les reprends ici pour rendre l'annexe "self contained" comme on dit...

Théorème 12 *Soit K un corps et V un sous-anneau de K ; sont équivalentes :*

1. *Le corps des fractions de V est K, et l'ensemble des idéaux de V est totalement ordonné pour la relation d'inclusion.*
2. *Le corps des fractions de V est K, et l'ensemble des idéaux principaux de V est totalement ordonné pour la relation d'inclusion.*
3. *Si $x \in K \setminus V$ alors $x^{-1} \in V$.*

Preuve — Il est évident que (1) implique (2). Supposons (2), et montrons (3) : soit $x \in K \setminus V$, alors $x = a/b$ avec $a, b \in K$. Puisque les idéaux monogènes de V sont totalement ordonnés, on a soit $\langle a \rangle \subset \langle b \rangle$ soit $\langle b \rangle \subset \langle a \rangle$. Comme $x \notin V$, la première inclusion est exclue ; c'est donc la deuxième qui est vérifée ce qui prouve que $x^{-1} \in V$. Il reste à montrer que (3) implique (1). Le fait que K soit le corps des fractions de V découle directement de (3). Soit I et J deux idéaux de V. On suppose que $I \not\subset J$, il existe donc $x \in I \setminus J$. Alors pour un quelconque $y \in J$, on a :

$$x \notin Vy \subset J \quad \Longrightarrow \quad \frac{x}{y} \notin V \quad \stackrel{(3)}{\Longrightarrow} \quad \frac{y}{x} \in V \quad \Longrightarrow \quad y \in Vx \subset I \ ;$$

de sorte que $J \subset I$. □

Définition 4 *Sous les hypothèses du théorème précédent, on dit que l'anneau V est un anneau de valuation pour le corps K. Plus généralement, on dit qu'un anneau V est un anneau de valuation s'il est intègre et si c'est un anneau de valuation pour son corps des fractions.*

Comme conséquences (assez directes) on peut déduire de la définition :

Propriété 3 *Soit V un anneau de valuation alors :*

1. *Parmi n éléments non nuls de V, il y en a un qui divise tous les autres.*
2. *L'anneau V est local. Notons $\mathfrak{m}(V)$ son idéal maximal.*
3. *Bien sûr V vérifie (3), mais plus précisément, si K est le corps des fractions de V, alors $x \in K \setminus V$ implique $x^{-1} \in \mathfrak{m}(V)$.*

[13]Même si, un amoureux de lecture, ne s'interdit pas de dévier de ce chemin tout tracé ; par exemple, une petite escapade à la fin ou encore une lecture en diagonale (comme on dit) soulage souvent la curiosité du lecteur assidu...

4. L'anneau V est intégralement clos.

Preuve — 1. Si $a_1, \ldots, a_n$ sont de tels éléments alors les idéaux $\langle a_1 \rangle, \ldots, \langle a_n \rangle$ étant totalement ordonnés, on a le résultat.

2. Les idéaux maximaux de V étant totalement ordonnés, V est nécessairement un anneau local.

3. Soit $x \in K \setminus V$. On sait que $x^{-1} \in V$. Si $x^{-1} \notin \mathfrak{m}(V)$, alors x^{-1} est inversible dans V car V est local ; par suite $x \in V$ ce qui est contradictoire.

4. Soit $x \in K$ entier sur V ; on a une relation de dépendance intégrale du type : $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ (avec $a_i \in V$ bien sûr). Supposons $x \notin V$. Alors $x^{-1} \in \mathfrak{m}(V)$. Ainsi :

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0 \quad \overset{\times x^{-n}}{\Longrightarrow} \quad 1 + \frac{a_{n-1}}{x} + \cdots + \frac{a_0}{x^n} = 0,$$

donc $1 \in \mathfrak{m}(V)$ ce qui est impossible. $\square$

De ces trois premières propriétés, on peut encore déduire sans trop d'effort les deux corollaires suivants :

Corollaire 16 *Soit K un corps et A un sous-anneau de K. On considère V un anneau de valuation pour K contenant A ; alors V contient la clôture intégrale de A dans K.*

Preuve — Soit $x \in K$ entier sur A. Alors x est a fortiori entier sur V donc élément de V car V est intégralement clos. $\square$

Avant d'énoncer un dernier résultat, j'ai besoin d'introduire une notion. La terminologie est malheureusement personnelle ; peut-être existe-t'il une terminologie universelle qui m'a échappée ???

Définition 5 *Soit A et B deux anneaux. L'anneau B est supposé local ; son idéal maximal est noté $\mathfrak{M}$. Je dis que B domine A si et seulement si A est un sous-anneau de B et $\mathfrak{M} \cap A$ est un idéal maximal de A.*

> **Remarque** – Si l'anneau A est lui aussi local, on retrouve la notion "classique" de domination entre anneaux locaux (c.f. [3], Chap 6, § 1, n°1).

Corollaire 17 *Soit K un corps et V un anneau de valuation pour K. Si B est un anneau **local** qui domine V alors $V = B$.*

Preuve — Comme B domine V, $V \subset B$. Il suffit donc d'assurer l'inclusion inverse. On note $\mathfrak{m}(V)$ et $\mathfrak{m}(B)$ les idéaux maximaux respectifs de V et B. Soit $x \notin V$, alors $x^{-1} \in \mathfrak{m}(V)$. Mais par définiton de la relation de domination, $\mathfrak{m}(V) = \mathfrak{m}(B) \cap V$. Par conséquent, $x^{-1} \in \mathfrak{m}(B)$ donc $x \notin B$, ce qu'il fallait montrer. $\square$

A.2 Prolongements de valuations

A.2.1 Le résultat général avec le langage des anneaux de valuation

La situation est la suivante : on dispose d'un anneau de valuation A, on note $\mathfrak{m}$ son idéal maximal et K son corps des fractions (que l'on suppose distinct de A). On considère L une extension **algébrique** de K de dimension finie égale à n ; soit B la fermeture intégrale de A dans L. En résumé :

$$\begin{array}{ccc} A & \xrightarrow{\text{clôt. int.}} & B \\ {\scriptstyle \text{Frac}}\downarrow & & \downarrow{\scriptstyle \text{Frac}} \\ K & \xrightarrow[\text{alg.}]{n} & L \end{array}$$

On commence par établir une proposition caractérisant les anneaux de valuation pour L dominant A. Ce résultat est un classique de la théorie des valuations (c.f. par exemple [14], Chap XII, §4, Proposition 4.8, ou évidemment [3], Chap 6, §8, n°6, Proposition 6) ; il est souvent énoncé tardivement dans les classiques (dans [3], il faut attendre le paragraphe 8[14] et il s'est déja passé une foule de choses...) alors que sa preuve ne nécessite pas plus de résultats que nous en avons déja.

Proposition 38 *Soit $\mathfrak{P}$ un idéal premier (non nul) de B ; alors le localisé $B_{\mathfrak{P}}$ est un anneau de valuation pour L qui contient A. De plus, la correspondance $\mathfrak{M} \mapsto B_{\mathfrak{M}}$ établit une bijection entre les idéaux maximaux de B et les anneaux de valuation pour L qui **dominent** A.*

[14] Le chapire 6 en comporte 10.

Remarque – En dimension 1, il n'y a pas lieu de distinguer les notions "contenir A" et "dominer A". Dans le cadre général, c'est fondamental. Pour s'en convaincre, il est bon de garder à l'esprit la remarque suivante : si V est un anneau de valuation pour un corps K, alors tout anneau V' contenant V et contenu dans K est encore un anneau de valuation pour K.

Avant d'établir ce résultat, montrons tout d'abord un lemme élémentaire valable dans tout anneau pour peu que ce dernier soit commutatif :

Lemme 22 *Soit A un anneau commutatif et x un élément d'un sur-anneau de A vérifiant une relation de dépendance algébrique du type :*

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \quad \textit{avec } a_i \in A. \tag{5}$$

Alors pour tout $k \in [1..n]$ on a :

1. *les éléments $r_k = a_n x^k + a_{n-1}x^{k-1} + \cdots + a_{n-k}$ sont entiers sur A ;*
2. *si x est de surcroît inversible dans le sur-anneau, il en est de même des éléments $s_k = a_0(x^{-1})^k + a_1(x^{-1})^{k-1} + \cdots + a_k$.*

Remarques

1. Pour $k = n$, le lemme nous apprend que $r_n = 0$ est entier sur A ; cela ne nous avance pas beaucoup même si ce résultat est tout à fait exact.

2. Pour $k = 1$, on retrouve une situation bien connue. En effet, $r_1 = a_n x + a_{n-1}$; or on sait bien que $a_n x$ est entier sur A donc a fortiori, r_1 l'est.

Preuve — Commençons par le premier point. Pour $k = 1$, comme on vient de le remarquer, c'est un résultat que l'on connaît bien. Il suffit en effet de multiplier la relation de dépendance, vérifiée par x, par a_n^{n-1} pour s'apercevoir que $a_n x$ est entier sur A et par suite qu'il en est de même pour $r_1 = a_n x + a_{n-1}$. Pour $k = 2$, on réécrit la relation de dépendance sous la forme :

$$(a_n x + a_{n-1})x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 = r_1 x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0 = 0.$$

Par suite, en réitérant le raisonnement précédent, on obtient que l'élément $r_1 x + a_{n-2}$ est entier sur $A[r_1]$ donc sur A par transitivité. Enfin, il est évident que $r_2 = r_1 x + a_{n-2}$. De proche en proche, en utilisant la relation $r_{i+1} = r_i x + a_{n-(i+1)}$, on montre bien que tous les r_i sont entiers sur A.

Pour le deuxième point, on remarque, en multipliant la relation (5) que x^{-1} vérifie la relation de dépendance algébrique sur A :

$$a_0 (x^{-1})^n + a_1 (x^{-1})^{n-1} + \cdots + a_{n-1}(x^{-1}) + a_n = 0$$

Il suffit pour conclure d'appliquer le premier point. $\square$

Preuve de la proposition 38 — • Soit $\mathfrak{P}$ un idéal premier de B. Commençons par montrer que le localisé $B_{\mathfrak{P}}$ est un anneau de valuation pour L. Pour cela, on considère x un élément de $L \setminus \{0\}$. Notre intention est de prouver que x ou $1/x$ appartient à $B_{\mathfrak{P}}$. Comme l'extension L/K est algébrique, il existe une relation de dépendance algébrique non triviale du type :

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0 \qquad \text{avec : } \quad a_i \in K$$

Quitte à multiplier par un élément non nul de A, on peut supposer que $a_i \in A$. Comme A est un anneau de valuation, l'un des a_i divise tous les autres. En simplifiant la relation de dépendance précédente par ce dernier ; on obtient (je ne change pas de notation, a_j/a_i est encore noté a_j ; de toutes façons, c'est la forme de la relation qui m'intéresse…) :

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

Je m'empresse de réécrire cette expression sous la forme :

$$\frac{a_n x^n + \cdots + a_{i+1}x^{i+1} + x^i}{x^i} + \frac{1}{x}\frac{a_{i-1}x^{i-1} + \cdots + a_0}{x^{i-1}} = y + \frac{1}{x}z = 0$$

avec :

$$y = a_n x^{n-i} + \cdots + a_{i+1}x + 1 \quad \text{et} \quad z = a_{i-1} + \cdots + a_0 x^{-(i-1)} = a_0(x^{-1})^{i-1} + \cdots + a_{i-1}$$

Examinons les expressions de y et z : on remarque que ces derniers sont respectivement les éléments r_{n-i} et s_{i-1} du lemme précédent obtenus à partir de la relation de dépendance algébrique de départ. Par suite, y et z sont entiers sur A c'est à dire éléments de B.

Pour conclure, on distingue deux cas : si $y \notin \mathfrak{P}$, alors en particulier y est non nul, et x se met sous la forme :

$$x = -\frac{z}{y} \qquad \text{avec} \quad z \in \mathfrak{P}, \quad y \in B \setminus \mathfrak{P}$$

c'est à dire $x \in B_{\mathfrak{P}}$. Dans le deuxième cas, c'est à dire si $y \in \mathfrak{P}$ ou encore si $y - 1 \notin \mathfrak{P}$ alors, il faut encore travailler un petit peu sur l'élément y. Ce dernier est par définition :

$$y = a_n x^{n-i} + \cdots + a_{i+1}x + 1 = 1 + x(a_n x^{n-i-1} + \cdots + a_{i+1}) = 1 + xy'$$

Mais y' est en fait l'élément r_{n-i-1} ; en conséquence, y' est entier sur A, i.e. élément de B. Ainsi, on a cette fois :

$$\frac{1}{x} = \frac{y'}{y-1} \qquad \text{avec} \quad y' \in B, \quad y - 1 \in B \setminus \mathfrak{P} \;;$$

autrement dit $1/x \in B_{\mathfrak{P}}$. Nous venons donc de montrer que nécessairement l'un des éléments x ou $1/x$ appartient à $B_{\mathfrak{P}}$, ce que l'on voulait.

• Montrons maintenant la deuxième partie de la proposition : soit $\mathfrak{M}$ un idéal maximal de B. On sait, d'après le premier point, que l'anneau $B_{\mathfrak{M}}$ est un anneau de valuation pour L qui contient A. Il reste à s'assurer, pour établir le premier sens de la correspondance, que $B_{\mathfrak{M}}$ domine A. En d'autres termes, il faut montrer que $\mathfrak{M}B_{\mathfrak{M}} \cap A = \mathfrak{m}$. Mais $\mathfrak{M}B_{\mathfrak{M}} \cap A = \mathfrak{M}B_{\mathfrak{M}} \cap B \cap A = \mathfrak{M} \cap A$; or, B est entier sur A, donc $\mathfrak{M} \cap A$ est un idéal maximal de A, c'est donc $\mathfrak{m}$, A étant local.

Réciproquement, soit V un anneau de valuation pour L qui domine A dont l'idéal maximal est noté $\mathfrak{m}(V)$. Alors, d'après le corollaire 16, $B \subset V$. De plus, comme V domine A, $\mathfrak{m}(V) \cap A = \mathfrak{m}$. Ainsi, l'idéal $\mathfrak{M}$ de B défini par $\mathfrak{M} = \mathfrak{m}(V) \cap B$ qui a priori n'est qu'un idéal premier de B est en fait maximal ; en effet, B est entier sur A et $\mathfrak{M} \cap A = \mathfrak{m}(V) \cap B \cap A = V \cap A = \mathfrak{m}$ qui est maximal. Par suite, V domine $B_{\mathfrak{M}}$ (ce sont deux anneaux locaux cette fois). Enfin, comme $B_{\mathfrak{M}}$ est un anneau de valuation pour L (on vient de le montrer), on a nécessairement $B_{\mathfrak{M}} = V$ d'après le corollaire 17. $\square$

A.2.2 Cette fois on prolonge des valuations, puis des valeurs absolues ultra-métriques

Prolongements de valuations :

Pour justifier le nom que porte cette section, "Prolongements de valuations", il nous reste à expliquer le lien entre la proposition 38 et le prolongement d'une valuation. Il suffit pour cela de se convaincre de l'équivalence pour un corps K entre la donnée d'un anneau de valuation pour K et d'une valuation (à équivalence près) sur K. Nous avons déjà évoqué le fait qu'une valuation sur K à valeurs réelles induise un anneau de valuation pour K, à savoir l'ensemble des éléments de K de valuation positive. Dans le cas général, i.e. quand la valuation est à valeurs dans un groupe commutatif **totalement ordonné**, il en est de même. Inversement, si A est un anneau de valuation pour K, d'idéal maximal $\mathfrak{m}$, alors on peut mettre une structure d'ordre total sur le groupe commutatif (multiplicatif) $K^*/U(A)$, à savoir : $x > y$ si et seulement si $x/y \in \mathfrak{m}$ (la relation d'ordre repose sur l'égalité $K^* = \mathfrak{m}^* \cup U(A) \cup \mathfrak{m}^{*-1}$, c.f. [14], Chap XII, §4 pour les détails ou encore et toujours [3], Chap 6, §3 n°2). L'application canonique $v : K^* \to K^*/U(A)$ que l'on prolonge à K en posant $v(0) = \infty$ définit alors une valuation sur K dont l'anneau de valuation associé n'est rien d'autre que l'anneau A. Le groupe $K^*/U(A)$, que l'on note souvent Γ_A, s'appelle le **groupe des ordres** de v ou de A.

Considérons maintenant A un anneau de valuation de corps des fractions égal à K, d'idéal maximal $\mathfrak{m}$, L une extension finie de K et enfin V un anneau de valuation pour L dominant A dont on note $\mathfrak{M}$ l'idéal maximal. Un petit schéma :

$$\begin{array}{ccc} A & \xrightarrow{\text{domination}} & V \\ {\scriptstyle\text{Frac}}\downarrow & & \downarrow{\scriptstyle\text{Frac}} \\ K & \xrightarrow[\text{finie}]{n} & L \end{array} \qquad\qquad \mathfrak{M} \cap A = \mathfrak{m}$$

Nous venons de voir que V est un localisé de B, la fermeture intégrale de A dans L, en un idéal maximal de B au dessus de $\mathfrak{m}$ (l'unique idéal maximal de A). On montre que le groupe des ordres de A, Γ_A, s'injecte dans celui de V noté Γ_V. En particulier, si w est la valuation sur L associée à l'anneau V (comme précédemment), l'injection précédente montre que w est un prolongement à L de v, la valuation sur K associée à l'anneau A. Je laisse désormais le soin à l'éventuel lecteur d'énoncer le pendant "valuationnel" de la proposition 38. En particulier, cela montre qu'étant donnée une valuation v sur un corps K, elle se prolonge à toute extension **finie** de K.

Prolongements de valeurs absolues ultra-métriques

Afin de pouvoir utiliser ce résultat pour établir l'existence du prolongement d'une valeur absolue, il reste encore un petit travail à faire.

> **Remarque** – Ce paragraphe est à mettre en rapport avec le passage de la section I.4.2, où il y était question de stratégies pour montrer l'existence du prolongement d'une valeur absolue à une extension algébrique.

On sait qu'étant donnée une valeur absolue ultra-métrique sur un corps K on peut lui faire correspondre une valuation à **valeurs réelles** via le logarithme. Le résultat concernant l'existence du prolongement des valuations sur un corps K à toute extension finie de K nous donnera celui concernant les valeurs absolues si toutefois on s'assure qu'une valuation à valeurs réelles se prolonge en une valuation à valeurs réelles ; plus extactement, si le groupe des ordres de la valuation "du bas" s'injecte dans $\mathbb{R}$, il faut montrer qu'il en est de même du groupe des ordres du prolongement.

Avant de s'en persuader, introduisons deux nouveaux invariants, l'indice et la dimension :

$$[\Gamma_V : \Gamma_A] \qquad \text{et} \qquad \dim_{A/\mathfrak{m}} V/\mathfrak{M}$$

Il est évident que la dimension $\dim_{A/\mathfrak{m}} V/\mathfrak{M}$ est finie car $\dim_{A/\mathfrak{m}} V/\mathfrak{M} \leqslant [L : K]$. L'indice $[\Gamma_V : \Gamma_A]$ est lui aussi fini et inférieur ou égal à $[L : K]$; en effet, considérons m éléments $x_1, \dots, x_m \in L^*$ tels que $w(x_i) \neq w(x_j) \pmod{\Gamma_A}$ et montrons qu'ils sont nécessairement K-linéairement indépendants. Soit $\sum \lambda_i x_i$ une combinaison K-linéaire non triviale ; on peut supposer qu'aucun des scalaires ne soit nul. Alors compte tenu de l'hypothèse, $w(\lambda_i x_i) \neq w(\lambda_j x_j) \pmod{\Gamma_A}$; mais alors $w(\sum \lambda_i x_i) = \min\{w(\lambda_i x_i)\} \neq \infty$, la combinaison linéaire est donc non triviale.

En fait, mieux que cela, on a l'inégalité (c.f.[14], Chap XII, §4, Proposition 4.6) :

$$[\Gamma_V : \Gamma_A] \times \dim_{A/\mathfrak{m}} V/\mathfrak{M} \leqslant \dim_K L$$

Il est grand temps d'indiquer les noms de ces deux entiers ; ils sont communément notés $e(w/v)$ et $f(w/v)$ respectivement :

- $e(w/v) = [\Gamma_V : \Gamma_A]$ s'appelle l'**indice de ramification** de w par rapport à v (ou de A dans V)
- $f(w/v) = \dim_{A/\mathfrak{m}} V/\mathfrak{M}$ s'appelle le **degré résiduel** de w par rapport à v (ou de A dans V).

Maintenant que nous avons montré la finitude de l'indice $[\Gamma_V : \Gamma_A]$, le fait qu'une valeur absolue à valeurs réelles se prolonge en une valeur absolue elle aussi à valeurs réelles découle directement du lemme suivant :

Lemme 23 *Soit Γ un groupe commutatif totalement ordonné et Γ' un sous-groupe de Γ tel que l'indice $[\Gamma : \Gamma']$ soit fini. Alors Γ s'injecte dans Γ' en tant que groupe ordonné.*

Preuve — Remarquons tout d'abord que Γ est sans torsion ; en effet, si $\gamma \neq 0$ et si par exemple $\gamma > 0$, alors $n\gamma > 0$ pour tout $n \in \mathbb{N}^*$ donc $n\gamma \neq 0$. Notons maintenant e l'indice $[\Gamma : \Gamma']$; alors l'application $\gamma \mapsto e\gamma$ est un morphisme injectif de Γ dans Γ' compatible avec la relation d'ordre. □

Cela étant, pour finir, nous allons polariser notre attention sur les degrés résiduels et indices de ramification introduits ci-avant. En particulier, intéressons nous désormais à la fameuse[15] relation $n = \sum e_i f_i$.

A.3 Autour de la relation $n = \sum e_i f_i$

Dans cette section, c'est le langage "anneaux de valuation" qui reprend "le dessus". Soit A un anneau de valuation de corps des fractions égal à K, d'idéal maximal $\mathfrak{m}$, L une extension finie de K et enfin B la clôture intégrale de A dans L. Considérons l'anneau $B/\mathfrak{m}B$. Tout d'abord, on montre que c'est une $A/\mathfrak{m}$-algèbre. En effet l'extension d'anneaux B/A étant entière, nécessairement $\mathfrak{m}B \neq B$ (c'est une conséquence du théorème du relèvement des idéaux premiers) ; par suite $\mathfrak{m}B \cap A = \mathfrak{m}$ et $B/\mathfrak{m}B$ est bien une $A/\mathfrak{m}$-algèbre. Mieux, c'est une $A/\mathfrak{m}$-algèbre de **dimension finie**. Cela repose sur la remarque simple suivante : dans un A-module

[15] tellement fameuse que Bourbaki, toujours dans [3], en fait même un titre de section : Chap 6, §8, n°5.

sans torsion (où A est un anneau de valuation bien sûr), dès que des vecteurs sont A-liés, l'un d'entre eux est combinaison linéaire des autres. Il suffit d'écrire la relation de dépendance linéaire et d'utiliser le fait que l'un des scalaires divise tous les autres. Considérons maintenant $n+1$ éléments de B (rappel : $n = [L : K]$) ; ils sont K liés donc A-liés, par suite l'un d'entre eux est combinaison linéaire des autres. En conséquence, dans le $A/\mathfrak{m}$-espace vectoriel $B/\mathfrak{m}B$, une famille constituée de plus de $n+1$ vecteurs est forcément liée ; ainsi :

$$\dim_{A/\mathfrak{m}} B/\mathfrak{m}B \leqslant n$$

Cette propriété est loin d'être anecdotique ; elle va nous permettre d'établir des résultats importants concernant l'anneau B et d'introduire de nouveaux invariants concernant l'extension L/K.

A.3.1 Une parenthèse, anneaux artiniens

Rappelons les principaux résultats concernant les anneaux artiniens à commencer par la définition :

Définition 6 *Un anneau A (commutatif unitaire) est dit artinien s'il vérifie l'une des conditions équivalentes suivantes :*

1. *l'anneau A est noethérien et de dimension nulle (i.e. tout idéal premier est maximal) ;*
2. *toute suite décroissante d'idéaux est stationnaire ;*
3. *en tant que A-module, l'anneau A est de longueur finie.*

Pour la preuve de l'équivalence de ces trois propriétés, je renvoie le lecteur à [16], Chap 9, §4. Mettons, dès à présent, en avant une catégorie d'anneaux artiniens : il s'agit des k-algèbres de **dimension finie** (où k un corps commutatif). En effet, soit A une telle algèbre ; c'est évidemment un anneau noethérien. Soit $\mathfrak{p}$ un idéal premier de A, alors la multiplication par un élément $x \in A/\mathfrak{p}$ non nul dans $A/\mathfrak{p}$ est k-linéaire injective donc bijective. Cela montre bien que tout élément non nul de $A/\mathfrak{p}$ y est inversible, d'où le résultat.

Attardons nous désormais sur la structure des anneaux artiniens :

Théorème 13 *Soit A un anneau artinien, il est semi local, i.e. il n'a qu'un nombre fini d'idéaux maximaux ; désignons ces derniers par $\mathfrak{m}_1 \dots \mathfrak{m}_k$, alors on a :*

1. *Chaque localisé $A_{\mathfrak{m}_i}$ est un anneau artinien local dans lequel l'idéal maximal $\mathfrak{m}_i$ est nilpotent.*
2. *Si ε_i est l'indice de nilpotence de l'idéal $\mathfrak{m}_i$ dans le localisé $A_{\mathfrak{m}_i}$, alors on a* ***dans ce localisé*** *:*

$$\{0\} = \mathfrak{m}_i^{\varepsilon_i} \subsetneq \mathfrak{m}_i^{\varepsilon_i - 1} \subsetneq \cdots \subsetneq \mathfrak{m}_i \subsetneq A_{\mathfrak{m}_i} \ ;$$

   de plus, ε_i est aussi le plus petit exposant tel que ***dans l'anneau*** *A on ait $\mathfrak{m}_i^{\varepsilon_i+1} = \mathfrak{m}_i^{\varepsilon_i}$.*

3. *Dans l'anneau A, on a l'égalité : $\mathfrak{m}_1^{\varepsilon_1} \cap \cdots \cap \mathfrak{m}_k^{\varepsilon_k} = \mathfrak{m}_1^{\varepsilon_1} \cdots \mathfrak{m}_k^{\varepsilon_k} = \{0\}$.*
4. *L'application canonique $A \to A_{\mathfrak{m}_i}$ induit un isomorphisme $A/\mathfrak{m}_i^{\varepsilon_i} \simeq A_{\mathfrak{m}_i}$, et par conséquent :*

$$A \simeq \prod_{i=1}^{k} A/\mathfrak{m}_i^{\varepsilon_i} \simeq \prod_{i=1}^{k} A_{\mathfrak{m}_i}$$

Preuve — Rappelons que dans un anneau noethérien, il n'y a qu'un nombre fini d'idéaux premiers minimaux ; or ici, à cause de la dimension 0, les ensembles suivants sont égaux :

$$\{\text{idéaux premiers minimaux}\} = \{\text{idéaux premiers}\} = \{\text{idéaux maximaux}\}$$

Ainsi, A est bien semi local ; notons $\mathfrak{m}_1, \dots, \mathfrak{m}_k$ ses idéaux maximaux alors : $\mathrm{Rad}(A) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k = \mathfrak{m}_1 \cdots \mathfrak{m}_k$. On sait aussi qu'il existe ε tel que $\mathrm{Rad}(A)^\varepsilon = 0$ (car A est nothérien) si bien que $\mathfrak{m}_1^\varepsilon \cdots \mathfrak{m}_k^\varepsilon = 0$. Il en résulte que dans chacun des localisés $A_{\mathfrak{m}_i}$, l'idéal maximal $\mathfrak{m}_i$ est nilpotent, d'indice de nilpotence, ε_i, inférieur ou égal à ε.

Cela étant, montrons maintenant que l'application canonique $A \to A_{\mathfrak{m}_i}$ induit un isomorphisme du quotient $A/\mathfrak{m}_i^{\varepsilon_i}$ sur le localisé $A_{\mathfrak{m}_i}$. Pour cela, on utilise le fait qu'il existe $t \in A$ tel que :

$$t \in \prod_{j \neq i} \mathfrak{m}_j^\varepsilon \qquad \text{et} \qquad t \notin \mathfrak{m}_i$$

si bien que $t \in A \setminus \mathfrak{m}_i$ et $t\mathfrak{m}_i^\varepsilon = 0$. Il en résulte déjà que $\mathfrak{m}_i^\varepsilon$ est inclu dans le noyau de l'application canonique $A \to A_{\mathfrak{m}_i}$. Réciproquement, si $x \in A$ est nul dans le localisé, alors il existe $s \in A \setminus \mathfrak{m}_i$ tel que $sx = 0$; comme s est inversible modulo $\mathfrak{m}_i^\varepsilon$, nécessairement $x \in \mathfrak{m}_i^\varepsilon$. Il reste à vérifier la surjectivité de l'application canonique ; il suffit de montrer que pour $s \in A \setminus \mathfrak{m}_i$ il existe $x \in A$ tel que $x = 1/s$. Comme s est inversible modulo $\mathfrak{m}_i$, il l'est modulo $\mathfrak{m}_i^\varepsilon$; autrement dit, il existe $x \in A$ tel que $xs \equiv 1 \pmod{\mathfrak{m}_i^\varepsilon}$ ou encore $t(xs-1) = 0$ i.e. $xs = 1$ dans le localisé. □

Le théorème précédent montre que l'on peut se contenter d'étudier les anneaux artiniens locaux.

Proposition 39 *Soit A un anneau artinien* ***local*** *d'idéal maximal $\mathfrak{m}$; dans toute suite de Jordan-Hölder de A, i.e. toute famille $I_1, \ldots, I_n$ d'idéaux tels que :*

$$\{0\} = I_n \subsetneq I_{n-1} \subsetneq \cdots \subsetneq I_1 \subsetneq I_0 = A \qquad \text{et} \qquad I_i/I_{i+1} \text{ est un } A\text{-module simple quelque soit } i$$

le quotient de deux termes consécutifs est un A-module isomorphe à $A/\mathfrak{m}$.

Preuve — La quotient de deux termes successifs I_{i+1}/I_i est un A-module simple ; c'est donc un A-module monogène engendré par x vérifiant : $A.x \simeq A/\operatorname{ann}(x)$. Pour satisfaire la condition de simplicité, il est nécessaire que l'idéal $\operatorname{ann}(x)$ soit maximal. Ici, compte tenu du caractère local de A, cela impose l'égalité $\operatorname{ann}(x) = \mathfrak{m}$; autrement dit, $A.x \simeq A/\mathfrak{m}$, ce que l'on voulait. □

En particulier, si A est une k-algèbre **locale** de dimension finie (k un corps commutatif, of course !), alors on a l'égalité dimensionnelle :

$$\dim_k A = l(A) \times \dim_k A/\mathfrak{m}$$

où $l(A)$ désigne la longueur de l'anneau A (i.e. l'entier n de la proposition précédente).

Remarques

1. Bien sûr, pour introduire la notion de longueur, il faut tout d'abord établir que deux suites de Jordan-Hölder de A ont la même longueur. Concernant ce résultat (c'est le théorème de Jordan) et tout ce qui concerne les suites de composition, je conseille la lecture de [24], Chap III, §11.

2. Attention, il semble que la terminologie concernant les suites de composition et de Jordan-Hölder, ne soit pas universelle. Je reprends ici la terminologie de Bourbaki (c.f.[4]) choisie aussi par Malliavin dans [16]. En revanche, pour Zariski et Samuel (loc. cit.), une suite de Jordan-Hölder est dénommée “composition series” et une suite de composition est appelée “normal series”.

Remarquons que dans le cadre des anneaux artiniens locaux, on dispose d'une suite de composition naturelle à savoir la suite décroissante des puissances de l'idéal maximal $\mathfrak{m}$:

$$\{0\} = \mathfrak{m}^\varepsilon \subsetneq \mathfrak{m}^{\varepsilon-1} \subsetneq \cdots \subsetneq \mathfrak{m} \subsetneq A$$

Bien sûr ε est l'indice de nilpotence de l'idéal $\mathfrak{m}$; notons de plus que cette suite est strictement décroissante à cause du lemme de Nakayama mais il n'y a aucune raison pour que cette suite soit de Jordan-Hölder. Pour qu'il en soit ainsi, il “ne faut pas de matière” entre deux puissances successives de $\mathfrak{m}$. On peut, cependant, affiner cette suite en une suite de Jordan-Hölder, ce qui montre l'inégalité : $\varepsilon \leqslant l(A)$. Il y a, tout de même, un cas où l'on peut montrer facilement l'égalité entre les deux entiers précédents ; il s'agit du cas où l'idéal $\mathfrak{m}$ est monogène. En effet, montrons à ce propos :

Lemme 24 *Soit A un anneau commutatif quelconque et $\mathfrak{m}$ un idéal maximal de A. Si $\mathfrak{m}$ est* ***monogène*** *alors soit $\mathfrak{m}^i/\mathfrak{m}^{i+1} = 0$ (i.e. $\mathfrak{m}^i = \mathfrak{m}^{i+1}$) soit $\mathfrak{m}^i/\mathfrak{m}^{i+1} \simeq A/\mathfrak{m}$.*

Preuve — Soit x un générateur de l'idéal $\mathfrak{m}$, si bien que $\mathfrak{m}^i = Ax^i$. L'application :

$$\begin{array}{rccc} \varphi : & A & \longrightarrow & \mathfrak{m}^i/\mathfrak{m}^{i+1} \\ & y & \longmapsto & yx^i \mod \mathfrak{m}^{i+1} \end{array}$$

est surjective ; son noyau contient l'idéal $\mathfrak{m}$, d'où le résultat. □

On déduit immédiatement de ce qui précède le corollaire :

Corollaire 18 *Soir k un corps et A une k-algèbre* ***locale*** *de dimension finie ; si l'unique idéal maximal de A, $\mathfrak{m}$, est* ***monogène*** *alors son indice de nilpotence, ε, est égal à la longueur de l'anneau A et on a l'égalité dimensionnelle :*

$$\dim_k A = \varepsilon \times \dim_k A/\mathfrak{m}$$

A.3.2 Anneaux artiniens et notre histoire

Revenons à l'anneau $B/\mathfrak{m}B$; c'est, comme nous l'avons déjà constaté, une $A/\mathfrak{m}$-algèbre de dimension finie. En particulier, $B/\mathfrak{m}B$ est donc artinien et par voie de conséquences noethérien et semi-local ; ses idéaux maximaux (en nombre fini donc) sont de la forme $\mathfrak{M}/\mathfrak{m}B$ où $\mathfrak{M}$ est un idéal maximal de B contenant $\mathfrak{m}$. En bref, il n'y a donc qu'un nombre fini d'idéaux maximaux de B au dessus de $\mathfrak{m}$. Autrement dit, compte tenu de la bijection mise en évidence dans le théorème 38, le nombre d'anneaux de valuation pour L **dominant** A est **fini**.

Cela étant, choisissons $\mathfrak{M}$ un idéal maximal de B au dessus de $\mathfrak{m}$. Tout d'abord, $\mathfrak{M}/\mathfrak{m}B$ est l'un des idéaux maximaux de l'anneau artinien $B/\mathfrak{m}B$; ce dernier est donc nilpotent (d'indice de nilpotence noté ε) dans le localisé :

$$(B/\mathfrak{m}B)_{\mathfrak{M}/\mathfrak{m}B} \simeq B_{\mathfrak{M}}/\mathfrak{m}B_{\mathfrak{M}}$$

L'anneau $B_{\mathfrak{M}}$ étant un anneau de valuation (c.f. théorème 38), l'ensemble de ces idéaux est totalement ordonné ; il en est donc de même de l'ensemble des idéaux du quotient $B_{\mathfrak{M}}/\mathfrak{m}B_{\mathfrak{M}}$. Par conséquent, ce dernier étant noethérien (il est même artinien), ces idéaux sont tous monogènes. En bref, $(B/\mathfrak{m}B)_{\mathfrak{M}/\mathfrak{m}B}$ est une $(A/\mathfrak{m})$-algèbre locale de dimension finie (au même titre que le quotient $B/\mathfrak{m}B$), dont l'idéal maximal est monogène ; en utilisant corollaire 18, on en déduit l'égalité :

$$\dim_{A/\mathfrak{m}}(B/\mathfrak{m}B)_{\mathfrak{M}/\mathfrak{m}B} = \dim_{A/\mathfrak{m}} B_{\mathfrak{M}}/\mathfrak{m}B_{\mathfrak{M}} = \varepsilon \times \dim_{A/\mathfrak{m}} B_{\mathfrak{M}}/\mathfrak{M}B_{\mathfrak{M}} = \varepsilon \times \dim_{A/\mathfrak{m}} B/\mathfrak{M}$$

Globalisons maintenant cette information : soient $\mathfrak{M}_1 \ldots \mathfrak{M}_g$ les idéaux maximaux de B au dessus de $\mathfrak{m}$, alors on a l'isomorphisme :

$$B/\mathfrak{m}B \simeq \prod_{i=1}^{g}(B/\mathfrak{m}B)_{\mathfrak{M}_i/\mathfrak{m}B} \simeq \prod_{i=1}^{g} B_{\mathfrak{M}_i}/\mathfrak{m}B_{\mathfrak{M}_i}$$

Désignant par ε_i l'indice de nilpotence de $\mathfrak{M}_i/\mathfrak{m}B$ dans le localisé $(B/\mathfrak{m}B)_{\mathfrak{M}_i/\mathfrak{m}B}$, on obtient l'égalité dimensionnelle (globale) :

$$\dim_{A/\mathfrak{m}} B/\mathfrak{m}B = \sum_{i=1}^{g} \varepsilon_i f_i \qquad \text{où on a posé :} \qquad f_i = \dim_{A/\mathfrak{m}} B/\mathfrak{M}_i$$

En résumé, nous venons d'établir le résultat suivant :

Proposition 40 *Soit A un anneau de valuation d'idéal maximal $\mathfrak{m}$, de corps des fractions K et L une extension finie de K. Alors il n'y a qu'un nombre fini d'anneaux de valuation pour L dominant A ; ce sont exactement les localisés de B, la fermeture intégrale de A dans L, par les idéaux maximaux $\mathfrak{M}_1, \ldots, \mathfrak{M}_g$ de B au dessus de $\mathfrak{m}$ (eux aussi en nombre fini).*

De plus, on a l'isomorphisme :

$$B/\mathfrak{m}B \simeq \prod_{i=1}^{g}(B/\mathfrak{m}B)_{\mathfrak{M}_i/\mathfrak{m}B} \simeq \prod_{i=1}^{g} B_{\mathfrak{M}_i}/\mathfrak{m}B_{\mathfrak{M}_i}$$

Pour chaque $1 \leqslant i \leqslant g$, l'idéal $\mathfrak{M}_i/\mathfrak{m}B$ est nilpotent dans le localisé $(B/\mathfrak{m}B)_{\mathfrak{M}_i/\mathfrak{m}B}$ d'indice de nilpotence ε_i ; enfin, on a l'égalité dimensionnelle :

$$\dim_{A/\mathfrak{m}} B/\mathfrak{m}B = \sum_{i=1}^{g} \varepsilon_i f_i \qquad \textit{où :} \qquad f_i = \dim_{A/\mathfrak{m}} B/\mathfrak{M}_i$$

A.3.3 Lien avec les définitions de Bourbaki

Les résultats de la section précédente figurent (évidemment !) dans le fameux sixième chapitre de la série Algèbre Commutative de Bourbaki (voir [3]) ; ils sont regroupés dans le §8 qui s'intitule : "Prolongement d'une valuation à une extension algébrique". Comme le suggère ce titre, le langage "valuationnel" y est de mise ; dans la section précédente nous parlions plutôt d'anneaux de valuation mais nous savons que cela revient au même.

Cela étant, revenons à la situation, désormais classique, suivante : on considère A un anneau de valuation de corps des fractions égal à K, L une extension finie de K et enfin V un anneau de valuation pour L dominant A. Un petit schéma :

$$\begin{array}{ccc} A & \xrightarrow{\text{domination}} & V \\ {\scriptstyle \text{Frac}}\downarrow & & \downarrow{\scriptstyle \text{Frac}} \\ K & \xrightarrow[\text{finie}]{n} & L \end{array}$$

Nous venons de voir que V est un localisé de B, la fermeture intégrale de A dans L, en un idéal maximal de B au dessus de $\mathfrak{m}$, l'unique idéal maximal de A. On sait que le groupe des ordres de A, Γ_A, s'injecte dans celui de V noté Γ_V. En particulier, si w est la valuation sur L associée à l'anneau V (comme précédemment), l'injection précédente montre que w est un prolongement à L de v. Nous avons introduit de plus $e = e(w/v) = [\Gamma_V : \Gamma_A]$ l'indice de ramification de w par rapport à v (ou de A dans V).

Et les entiers ε introduits dans la section précédente, que sont-ils ? Le maître Bourbaki les dénomment **indice initial de ramification** de w par rapport à v. La définition qu'il en donne n'a rien à voir (a priori) avec celle liée aux indices de nilpotence ; cela s'explique (peut-être) par le souhait de donner une définition uniquement en terme de valuation, la rendant ainsi beaucoup plus intrinsèque. Ce faisant, Bourbaki, dans [3], Chap 6, §8, n°4 et 5, démontre évidemment toutes les propriétés relatives aux ε que l'on a énoncées ci-avant et d'autres encore. Par exemple on peut y lire que ε divise e. Retrouvons cette relation de divisibilité à partir de la définition de ε précédemment choisie : si $\varepsilon = 1$, il n'y a rien à faire ; on se place dans le cas où $\varepsilon > 1$. Pour établir la relation de divisibilité avancée, nous allons établir le lemme intermédiaire suivant :

Lemme 25 *On conserve les hypothèses précédentes et on suppose de plus que* $\mathfrak{m}V \subsetneq \mathfrak{M}$. *Soit* $x \in \mathfrak{M}$ *tel que* $x \pmod{\mathfrak{m}V}$ *engendre l'idéal* $\mathfrak{M}/\mathfrak{m}V$ *du quotient* $V/\mathfrak{m}V$ *; alors l'ordre de la classe de* $x \mod U(V)$ *dans le groupe quotient (multiplicatif)* Γ_V/Γ_A *est égal à l'indice de nilpotence de* $x \mod \mathfrak{m}V$ *dans l'anneau quotient* $V/\mathfrak{m}V$.

Montrons, avant d'établir ce résultat, que la relation de divisibilité précédente en découle. Tout d'abord, nous avons déjà constaté que l'idéal $\mathfrak{M}/\mathfrak{m}V$ du quotient $V/\mathfrak{m}V$ est monogène, ce qui montre l'existence de l'élément x ; l'indice de nilpotence de $x \pmod{\mathfrak{m}V}$ dans le quotient $V/\mathfrak{m}V$ n'est rien d'autre que ε l'indice initial de ramification de w par rapport à v. L'hypothèse supplémentaire $\mathfrak{m}V \subsetneq \mathfrak{M}$ est équivalente à $\varepsilon \geqslant 2$. Nous voulons montrer que ε divise e. Si $\varepsilon = 1$, il n'y a rien à montrer. On se place dans le cas contraire, ce qui nous permet d'utiliser le lemme précédent. L'indice de nilpotence de $x \mod \mathfrak{m}V$ dans l'anneau quotient $V/\mathfrak{m}V$, à savoir ε est donc égal à l'ordre de la classe de $x \mod U(V)$ dans le groupe Γ_V/Γ_A ; ce dernier étant d'ordre e, on a le résultat.

Preuve du lemme 25 — Commençons par faire deux remarques indépendantes de l'hypothèse $\mathfrak{m}V \subsetneq \mathfrak{M}$.

Tout d'abord, par définition, le groupe Γ_V/Γ_A est un quotient de L^*. En fait, on vérifie aisément que :

$$\Gamma_V/\Gamma_A \simeq L^*/U(V)K^*$$

On voit donc apparaître le sous-groupe de L^*, $U(V)K^*$.

Ensuite, on a les inclusions suivantes :

$$\mathfrak{m}V \setminus \mathfrak{m}\mathfrak{M} \subset U(V)K^* \cap \mathfrak{M} \subset \mathfrak{m}V$$

Soit $y \in \mathfrak{m}V$; alors $y \in \mathfrak{M}$ (car $\mathfrak{m}V \subset \mathfrak{M}$) et on peut écrire :

$$y = \sum_{\text{finie}} m_i \xi_i \qquad \text{avec :} \quad m_i \in \mathfrak{m} \text{ et } \xi_i \in V$$

Puisque A est un anneau de valuation, l'un des m_i divise tous les autres, notons le m ; en le mettant en facteur dans la somme précédente, cette dernière se ré-écrit sous la forme : $y = m\xi$ avec $\xi \in V$. Par ailleurs, comme $y \notin \mathfrak{m}\mathfrak{M}$, nécessairement $\xi \notin \mathfrak{M}$, i.e. $\xi \in V \setminus \mathfrak{M} = U(V)$. Nous venons donc de montrer que $y \in U(V)K^*$. Le reste ne pose aucun problème.

Cela étant, revenons à la démonstration du lemme proprement dit. Utilisons cette fois l'hypothèse $\mathfrak{m}V \subsetneq \mathfrak{M}$: par définition de x,

$$\mathfrak{M}/\mathfrak{m}V = (V/\mathfrak{m}V).\overline{x} \qquad \text{si bien que} \qquad \mathfrak{M} = \mathfrak{m}V + Vx$$

L'anneau V étant de valuation, soit $\mathfrak{m}V \subset Vx$, soit $Vx \subset \mathfrak{m}V$; dans le premier cas $\mathfrak{M} = Vx$, dans le second $\mathfrak{M} = \mathfrak{m}V$. Comme ce dernier est exclu, par hypothèse, nécessairement $\mathfrak{M} = Vx$.

Tout est prêt pour conclure désormais. On note α l'ordre de la classe de $x \mod U(V)$ dans le groupe quotient Γ_V/Γ_A. Compte tenu de l'isomorphisme de groupe rappelé plus haut, $x^\alpha \in U(V)K^*$; comme de plus, $x \in \mathfrak{M}$, $x^\alpha \in U(V)K^* \cap \mathfrak{M} \subset \mathfrak{m}V$. Ceci montre que $\varepsilon \leqslant \alpha$. Inversement, par définition de ε, $x^\varepsilon \in \mathfrak{m}(V)$ et $x^{\varepsilon-1} \notin \mathfrak{m}(V)$; ainsi (en multipliant par x) $x^\varepsilon \notin \mathfrak{m}Vx$, i.e. $x^\varepsilon \notin \mathfrak{m}\mathfrak{M}$. En bref, $x^\varepsilon \in \mathfrak{m}V \setminus \mathfrak{m}\mathfrak{M} \subset U(V)K^*$; cela assure l'inégalité inverse, $\alpha \leqslant \varepsilon$. □

En particulier, on a toujours l'inégalité $\varepsilon \leqslant e$ (cela peut se montrer directement, en remarquant que $x^e \in \mathfrak{m}V$). Cette inégalité peut être stricte. Je donne un exemple qui m'a été inspiré par la lecture d'un exercice de Bourbaki : [3], Chap 6, §8, exercice 4 (quelle mine d'informations que ces exercices !). On se place dans le corps $L = k(X,Y)$ (où k est un corps commutatif) que l'on muni de la valuation w à valeurs dans $\mathbb{Z} \times \mathbb{Z}$ ordonné lexicographiquement et définie par :

$$w(X) = (1,0) \qquad \text{et} \qquad w(Y) = (0,1)$$

Le groupe des ordres de w, Γ_w, est égal à $\mathbb{Z} \times \mathbb{Z}$. Considérons la sous-extension $K = k(X^2, Y)$ et notons v la restriction de w à ce corps :

$$K = k(X^2,Y) \overset{n=2}{\text{———}} k(X,Y) = L$$

Le groupe des ordres de v est évidemment $2\mathbb{Z} \times \mathbb{Z}$ ce qui montre que $e = e(w/v) = [\mathbb{Z} \times \mathbb{Z} : 2\mathbb{Z} \times \mathbb{Z}] = 2$. Nous allons vérifier que $\varepsilon = \varepsilon(w/v) = 1$. Il s'agit donc de prouver que $\mathfrak{m}V = \mathfrak{M}$ ou encore $\mathfrak{M} \subset \mathfrak{m}V$. Cela repose sur le fait que $w(Y)$ est de valuation **strictement positive minimum**. Autrement dit, Y divise tous les éléments de $\mathfrak{M}$. Par suite, si $R \in \mathfrak{M}$, l'écriture :

$$R(X,Y) = Y \times \frac{R(X,Y)}{Y} \qquad \text{où :} \quad Y \in \mathfrak{m} \quad \text{et} \quad \frac{R(X,Y)}{Y} \in V$$

assure l'inclusion $\mathfrak{M} \subset \mathfrak{m}V$, ce que l'on voulait.

Remarque – Comme $n = 2$, avec des notations implicites, on a $f = 1$ car on sait que $ef \leqslant n$. En fait, les deux corps résiduels sont isomorphes à k (c.f.[3], Chap 6, §3, n°4, Exemple 6).

En revanche, dans le cas discret, de tels phénomènes ne se produisent pas ; autrement dit, on a toujours l'égalité $e = \varepsilon$. En effet, si l'anneau V est de plus principal (ce qui revient à dire que la valuation w est discrète), alors on peut choisir $x \in V$ de telle sorte qu'il engendre l'idéal $\mathfrak{M}$ (x est une uniformisante de w). La divisibilité est alors la plus simple possible (hormis celles des corps !), à savoir :

$$V^* = U(V)x^{\mathbb{N}} \qquad \text{et} \qquad L^* = U(V)x^{\mathbb{Z}}$$

Le groupe Γ_V, lui, est cyclique engendré par $w(x)$.

Revenons à la situation précédente, comme Γ_V est engendré par $w(x)$, l'ordre de $x \mod U(V)$ est égal à e.

- Si $\varepsilon \geqslant 2$, d'après le lemme précédent, cet ordre est aussi égal à ε, d'où l'égalité dans ce cas particulier.
- Il reste à vérifier que $\varepsilon = 1$ implique $e = 1$ (ce qui n'est pas toujours vrai comme l'illustre l'exemple précédent). Mais si $\varepsilon = 1$ alors $\mathfrak{m}V = \mathfrak{M}$; par suite, si $\mathfrak{m} = Ax$ alors $\mathfrak{M} = Vx$, si bien que $L^* = U(V)x^{\mathbb{Z}}$ avec $x \in K^*$. Autrement dit, tout élément $y \in L^*$ appartient à $U(V)K^*$; cela montre bien que $e = 1$, ce que l'on voulait.

En résumé, nous venons de montrer que :

Proposition 41 *Soit K un corps, L une extension finie de K, w une valuation sur L et v sa restriction à K. Alors l'indice initial de ramification de w par rapport à v divise l'indice de ramification de w par rapport à v et lui est égal si w est discrète.*

Pour terminer, je cite (pour la démonstration, je renvoie le lecteur à [3], Chap 6, §8, n°5, théorème 2) l'un des derniers résultats très importants concernant ce sujet, à savoir :

Théorème 14 *Soit K un corps muni d'une valuation v d'anneau A d'idéal maximal $\mathfrak{m}$, L une extension finie de K de degré n, B la fermeture intégrale de A dans L et $v_1, \ldots, v_g$ un système complet de prolongements de v à L, alors les conditions suivantes sont équivalentes :*

1. *l'anneau B est un A-module de type fini ;*
2. *l'anneau B est un A-module libre ;*
3. *on a $[B/\mathfrak{m}B : A/\mathfrak{m}A] = n$;*
4. *on a $\sum_{1\leqslant i\leqslant g} e(v_i/v)f(v_i/v) = n$ et $e(v_i/v) = \varepsilon(v_i/v)$ pour tout i.*

References

[1] Abhyankar, S. S. Galois Theory on the Line in NonZero Characteristic. *Bulletin of the American Mathematical Society Vol. 27*, 1 (1992).

[2] Borevitch, Z. I., and Chafarevitch, I. *Théorie des nombres.* Gauthier-Villars Paris, 1967.

[3] Bourbaki, N. *Algèbre Commutative, chapitres 5 et 6.* Hermann, 1961.

[4] Bourbaki, N. *Algèbre, chapitre 1.* Hermann, 1964.

[5] Bourbaki, N. *Algèbre, chapitres 4 à 7.* Masson, 1981.

[6] Cassels, J. W. S., and Frohlich, A. *Algebraic Number Theory.* Academic Press, 1967. Proceedings of an instructional conference.

[7] Cohen, H. *A Course in Computational Algebraic Number Theory.* Springer, 1995.

[8] Dieudonné, J. *Eléments d'analyse 1*, troisième ed. gauthier-villars, 1969.

[9] Dieudonné, J. *Abrégé d'histoire des mathématiques 1700-1900.* Hermann, 1978. sous la direction de J.Dieudonné avec la collaboration d'autres auteurs.

[10] Frohlich, A., and Taylor, M. J. *Algebraic Number Theory.* Cambridge University Press, 1991.

[11] Huppert, B., and Blackburn, N. *Finite Groups III.* Springer-Verlag, 1982.

[12] Kondo, T. Algebraic number fields with the discriminant equal to that of a quadratic number field. *J.Math.Soc. Japan Vol. 47*, 1 (1995).

[13] Lang, S. *Number theory.* Addison Wesley, 1970.

[14] Lang, S. *Algebra*, Third ed. Addison Wesley, 1994.

[15] Malle, G., and Matzat, B. H. *Inverse Galois Theory.* Preprint, Université Heidelberg, 1992.

[16] Malliavin, M.-P. *Algèbre commutative.* Masson, 1985.

[17] Narkiewicz, W. *Elementary and analytic theory of algebraic numbers*, second ed. Polish Scientific Publishers, 1990.

[18] Naudin, P., and Quitté, C. *Algorithmique Algébrique.* Masson, 1992.

[19] Naudin, P., and Quitté, C. *Cours de DEA 1993-1994 : Algorithmique en théorie des corps.* Prépublication de l'Université de Poitiers, 1994.

[20] Samuel, P. *Théorie algébrique des nombres*, deuxième ed. Hermann, 1971.

[21] Serre, J.-P. *Corps locaux*, troisième ed. Hermann, 1968.

[22] Serre, J.-P. *Topics in Galois theory.* Jones and Barlett Publishers, Boston, 1992.

[23] Weiss, E. *Algebraic Number Theory.* McGraw-Hill, 1963.

[24] Zariski, O., and Samuel, P. *Commutative Algebra Vol 1.* Springer-Verlag, 1958.