Théorème de Skolem et analyse p-adique

Alban PIROUTET

Mai-Juin 2024

Remerciements

Je remercie tout d'abord Olivier Fouquet mon maître de stage pour avoir accepté de m'encadrer, m'avoir fait découvrir des personnalités et chercheurs/chercheurses extrêmements intéressants, Rafik Souanef pour ses conseils et explications de la théorie de Galois, l'équipe doctorale pour sa gentillesse et leur goût à la recherche.

Table des matières

Introduction

Introduit par Hensel dans le but d'appliquer la théorie des séries formelles au nombre milieu du XIX ème siècle l'analyse p-adique a permis la démonstration de nombreux théorèmes dont le théorème de Skolem, un outil puissant dans l'étude des suites définies par une relation de récurrence linéaire. Sa démonstration nécessite l'analyse p-adique et la question d'une preuve sans l'utilisation de cette dernière reste encore un problème ouvert. Ainsi ce domaine des mathématiques semble être crucial dans la résolution de problèmes faisant intervenir les entiers et nous essayerons dans cet écrit de couvrir les points importants de cette théorie. De plus nous étudierons la théorie de Galois, une théorie très important des mathématiques, très puissante notament en algèbre.
Pour l'entièreté de l'écrit, p désigne un nombre premier.

1 Corps muni d'une valeur absolue

On se propose d'étudier quelques résultats classiques sur les corps et en particulier ceux munis d'une valeur absolue.

1.1 Définitions et premières propriétés

Définition 1. *Soit $\mathbb{K}$ un corps, une* ***valeur absolue sur*** $\mathbb{K}$ *est une fonction*

$$|.| : \mathbb{K} \to \mathbb{R}^+$$

qui vérifie :

i) $|x| = 0 \iff x = 0$

ii) $|xy| = |x||y|$, $\forall x, y \in \mathbb{K}$

iii) $|x + y| \leq |x| + |y|$, $\forall x, y \in \mathbb{K}$

Une valeur absolue est dite ***ultramétrique*** *ou* ***non-archimédienne*** *lorsqu'elle vérifie aussi*

$$\forall x, y \in \mathbb{K},\ |x + y| \leq max(|x|, |y|)$$

Dans le cas contraire, elle est dite ***archimédienne****.*

Lemme 1. *Soit $|.|$ une valeur absolue sur un corps $\mathbb{K}$. On a :*

i) $|1| = 1$

ii) Si $x \in \mathbb{K}$ et $n \in \mathbb{N}$ tels que $|x^n| = 1$ alors $|x| = 1$.

iii) $|-1| = 1$

iv) Pour tout $x \in \mathbb{K}$, $|-x| = |x|$

v) Si $\mathbb{K}$ est un corps fini, $|.|$ est trivial ie $|0| = 0$ et $\forall x \in \mathbb{K}^*, |x| = 1$.

Théorème 1. *Soit $A \subset \mathbb{K}$ l'image de $\mathbb{Z}$ dans $\mathbb{K}$. Une valeur absolue sur $\mathbb{K}$ est non-archimédienne si et seulement si $|a| \leq 1, \forall a \in A$.*

Démonstration. Sens direct : Soit $|.|$ une valeur absolue non-archimédienne sur $\mathbb{K}$, on a $\forall a \in A$, $|a \pm 1| \leq \max(|a|, 1)$ donc par récurrence on en déduit que $\forall a \in A, |a| \leq 1$.
Pour le sens réciproque : On suppose que $\forall a \in A, |a| \leq 1$. On veut montrer que $\forall x, y \in \mathbb{K}, |x + y| \leq \max(|x|, |y|)$. On remarque que si $y = 0$ le résultat est clair, dans le cas contraire on peut diviser par $|y| > 0$ et on doit montrer que $|1 + \frac{x}{y}| \leq \max(1, |\frac{x}{y}|)$. Il suffit donc de prouver que $\forall x \in \mathbb{K}, |1 + x| \leq \max(1, |x|)$. Soit $m \in \mathbb{N}$, on a $|(1 + x)^m = \sum_{n=0}^m \binom{m}{n} x^n| \leq \sum_{n=0}^m |\binom{m}{n} x^n| \leq \sum_{n=0}^m |\binom{m}{n}||x^n| \leq \sum_{n=0}^m |x^n|$ car les coefficients binômiaux sont entiers. Ainsi on a

$$|\sum_{n=0}^{m} \binom{m}{n} x^n| \leq (m + 1)\max(1, |x|^m)$$

En passant à la racine m-ième on a que $|1 + x| \leq \max(1, |x|)(1 + m)^{\frac{1}{m}}$ avec le terme de droite qui tend vers 1 lorsque m tend vers $+\infty$ d'où le résultat par passage à la limite.

Proposition 1. *Une valeur absolue $|.|$ sur le corps $\mathbb{K}$ est archimédienne si pour $x, y \in \mathbb{K}, x \neq 0$ il existe $n \in \mathbb{N}$ tel que $|nx| > |y|$.*

Théorème 2. *Une valeur absolue $|.|$ est non-archimédienne si et seulement si $sup(|n|, n \in \mathbb{Z}) = 1$.*

1.2 Topologie

La première chose est de mesurer les choses et pour cela nous avons besoin d'introduire une distance :

Définition 2. *Soit $\mathbb{K}$ un corps muni d'une valeur absolue $|.|$, on définit la distance sur $\mathbb{K}$ associé à $|.|$ par :*

$$\forall x, y \in \mathbb{K}, d(x, y) = |x - y|$$

Par les propriétés de $|.|$, on vérifie facilement que d vérifie :

i) $\forall x, y \in \mathbb{K}, d(x, y) \geq 0$ *et* $d(x, y) = 0 \iff x = y$.

ii) $\forall x, y \in \mathbb{K}, d(x, y) = d(y, x)$

iii) $\forall x, y, z \in \mathbb{K}, d(x, y) \leq d(x, z) + d(z, y)$

Ce sont en fait les axiomes de la définition d'une distance !

Proposition 2. *Un corps $\mathbb{K}$ muni d'une valeur absolue est un* ***corps topologique*** *i.e la multiplication, l'addition et l'inverse sont des opérations* ***continues****.*

Lemme 2. *Soit $(\mathbb{K}, |.|)$ un corps muni d'une valeur absolue alors $|.|$ est non-archimédienne si et seulement si*

$$\forall x, y, z \in \mathbb{K} d(x, y) \leq max(d(x, z), d(y, z))$$

Démonstration. Le sens direct est clair, il suffit d'ajouter z artificiellement et d'appliquer l'inégalité triangulaire. Pour le sens réciproque il suffit de considérer $-y$ et $z = 0$.

Proposition 3. *Soit $\mathbb{K}$ un corps muni d'une valeur absolue* ***non-archimédienne*** *alors:*

$$\forall x, y \in \mathbb{K} : |x| \neq |y| \implies |x \pm y| = \max(|x|, |y|).$$

Démonstration. Comme $|.|$ est non-archimédienne, on a que $|x \pm y| \leq \max(|x|, |y|)$. Puis si $|x| \neq |y|$ quitte à échanger les rôles de x et y, on peut supposer que $|x| < |y|$. Puis on a $|y| = |y - x + x| \leq max(|y - x|, |x|)$ or par hypothèse $|y| > |x|$ donc l'inégalité impose que $|y| \leq |y - x|$. On a donc $|y| = \max(|x|, |y|) \leq |y - x|$ d'où le résultat.

Etudier un ensemble en général revient à étudier sa topologie, on introduit donc le vocabulaire nécessaire:

Définition 3. *Soit $\mathbb{K}$ un corps muni d'une valeur absolue, soit $x \in \mathbb{K}$ et $r \geq 0$ on définit :*

- *La boule ouverte de centre x et de rayon r l'ensemble $B(x, r) = \{y \in \mathbb{K}, |x - y| < r\}$*
- *La boule fermée de centre x et de rayon r l'ensemble $\bar{B}(x, r) = \{y \in \mathbb{K}, |x - y| \leq r\}$*

Les valeurs absolues non-archimédiennes possèdent un comportement bien différent de celui par exemple de la valeur absolue classique sur $\mathbb{R}$ en effet on observe ces résultats surprenants :

Proposition 4. *Soit $\mathbb{K}$ un corps muni d'une valeur absolue $|./|$* ***non-archimédienne*** *alors :*

- *Tout point appartenant à une boule ouverte en est le centre.*
- *Tout point appartenant à une boule fermée en est le centre.*
- *Les boules ouvertes sont aussi fermées*
- *Si $r > 0$ alors $\forall x \in K$, $\bar{B}(x, r)$ est ouverte.*
- *Deux boules ouvertes sont soit disjointes soit égales.*
- *Deux boules fermées de rayons strictement positifs sont soit égales soit disjointes.*

Proposition 5. *Soit $\mathbb{K}$ un corps muni d'une valeur absolue $|./|$* ***non-archimédienne*** *alors la composante connexe de chaque élément est le singleton égale à ce-dernier.*

2 Corps p-adiques

2.1 Construction topologique du corps p-adique $\mathbb{Q}_p$

2.1.1 Motivation

Le corps des rationnels $\mathbb{Q}$ n'est pas complet en effet on peut construire une suite de Cauchy rationnelle qui ne converge pas dans $\mathbb{Q}$. De même $\mathbb{Q}$ n'est pas complet pour la valeur absolue p-adique. Ainsi certaines suites qui devraient converger n'ont au final peut-être pas de limite. Ainsi nous allons construire $\mathbb{Q}_p$ comme une extension de $\mathbb{Q}$ de manière que les suites qui devraient converger ont une limite. La construction de ce nouvel objet est similaire à celle de la construction de $\mathbb{R}$.

Définition 4. *Soit $a \in \mathbb{Z}$ on définit la* ***valuation p-adique de*** *a par $v_p(a)$=l'exposant de p dans la décomposition en produit de facteurs premiers de n.*
On étend cette notion à $\mathbb{Q}$. Si $r = \frac{a}{b}$ est un rationnel, on pose $v_p(r) = v_p(a) - v_p(b)$. Ceci ne dépend pas du représentant $\frac{a}{b}$ choisi. Ainsi $r = p^{v_p(r)}\frac{u}{v}$ avec $u, v \in \mathbb{Z}$ et $p \nmid uv$. On adopte la convention $v_p(0) = +\infty$, seul zéro est divisible par toutes les puissances de p.

Définition 5. *On définit donc la valeur absolue p-adique par :*

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

Avec la convention $|0|_p = 0$

Proposition 6. *La valeur absolue p-adique est* ***ultramétrique****.*

Définition 6. *On définit les ensembles* $\mathcal{C}_p(\mathbb{Q}) := \{(x_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}} \mid \forall \epsilon \in \mathbb{Q}_+^*, \exists N_\epsilon > 0 \mid \forall (n,m) \in \mathbb{N}^2, n,m > N_\epsilon \Rightarrow |x_n - x_m|_p < \epsilon\}$ *et* $\mathcal{N} := \{(x_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}} \mid \lim_{n\to+\infty} x_n = 0\}$.

Proposition 7. $\mathcal{N}$ *est un idéal maximal de* $\mathcal{C}_p(\mathbb{Q})$.

Démonstration. Il est clair que $\mathcal{N}$ est un idéal de $\mathcal{C}_p(\mathbb{Q})$ en effet une suite convergente est de Cauchy, la suite nulle est convergente de limite nulle, la différence de suites de limite nulle est encore convergente de limite nulle. De plus toute suite de Cauchy est bornée donc son produit par une suite convergente vers 0 est convergent de limite 0. Montrons que le caractère maximal de cet idéal :

Lemme 3. *1) Si* $(x)_{n\in\mathbb{N}} \in \mathcal{C}_p(\mathbb{Q})\backslash\mathcal{N}$ *alors la suite de terme général* $|x_n|_p$ *est constante à partir d'un certain rang.*
2) Si $a = (a)_{n\in\mathbb{N}}$ *et* $b = (b)_{n\in\mathbb{N}}$ *sont deux éléments de* $\mathcal{C}_p(\mathbb{Q})$ *différant par un élément de* $\mathcal{N}$*,alors* $\lim_{n\to\infty} |a_n|_p = \lim_{n\to\infty} |b_n|_p$

1)Si $(x)_{n\in\mathbb{N}} \in \mathcal{C}_p(\mathbb{Q})\backslash\mathcal{N}$ il existe alors $\delta > 0$ tel que pour une infinité de n on est $|x_n|_p \geq \delta$. La limite est donc supérieure à δ et donc comme la suite est de Cauchy $\exists N \in \mathbb{N}$ tel que $\forall n \geq \mathbb{N}, |a_n|_p \geq \frac{2}{3}\delta$ et $|a_{n+p} - a_n|_p < \frac{\delta}{2}$. On a donc $|a_{n+p} - a_n|_p < |a_n|_p$ comme $|.|_p$ est ultramétrique on a $|a_{n+p}|_p = |a_n|_p$.
2) On a $||a_n|_p - |a_n|_p|_p \leq |a_n - b_n|_p$ qui tend bien vers 0 d'où le résultat.

Retour à notre première démonstration : Si $x = (x)_{n\in\mathbb{N}} \in \mathcal{C}_p(\mathbb{Q})\backslash\mathcal{N}$, d'après ce qui précède, il existe $\delta > 0$ et $N \in \mathbb{N}$ tels que l'on ait $|a_n|_p > \delta$ pour $n \geq N$. La suite $b = (b)_{n\in\mathbb{N}}$ définie par $b_n = 0$ si $n < N$ et $b_n = {a_n}^{-1}$ si $n \geq N$ est de Cauchy et $ab - 1$ appartient à $\mathcal{N}$, ce qui montre que $\bar{a}$ est inversible dans $\mathcal{C}_p(\mathbb{Q})/\mathcal{N}$ donc $\mathcal{C}_p(\mathbb{Q})/\mathcal{N}$ est un corps donc $\mathcal{N}$ est maximal.

Définition 7. *On définit la relation d'équivalence* $\sim$ *sur* $\mathbb{C}_p$ *par :*

$$(x)_{n\in\mathbb{N}} \sim (y)_{n\in\mathbb{N}} \iff \lim_{n\to\infty} |x_n - y_n|_p = 0$$

Définition 8. *On définit* $\mathbb{Q}_p$ *par* $\mathbb{Q}_p := \mathcal{C}_p(\mathbb{Q})/\sim = \mathcal{C}_p(\mathbb{Q})/\mathcal{N}$

Proposition 8. $\mathbb{Q}_p$ *est un corps et* $\mathbb{Q}$ *s'injecte dedans.*

Démonstration. Le lemme précédent assure que $\mathbb{Q}_p$ est un corps et $\mathbb{Q}$ s'injecte dedans en effet pour tout rationnel q on considère la suite $x = (q)_{n\in\mathbb{N}}$ qui est bien de Cauchy (pour $|.|_p$) car constante.

Définition 9. *On étend la définition de la valuation à* $\mathbb{Q}_p$ *en posant :*

$$v_p(a) = \begin{cases} \lim_{n\to\infty} |a_n|_p & \text{si } a \neq 0 \\ +\infty & \text{sinon} \end{cases}$$

Cela ne dépend pas du représentant choisi d'après le 2) du Lemme 3.

Définition 10. *Soit* $a \in \mathbb{Q}_p$ *on définit :* $|a|_p = 0$ *si* $a = 0$ *et* $|a|_p = p^{-v_p(a)}$ *sinon. On définit aussi* $d_p(a,b) = |a - b|_p$ *pour tout* $a, b \in \mathbb{Q}_p$.

Proposition 9. *Formule du produit : Soit $x \in \mathbb{Q}^*$. On a $\Pi_{p\leq\infty}|x|_p = 1$.*

Démonstration. Il suffit de prouver le résultat lorsque x est un entier positif. Si $x = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. On a alors :

$$\begin{cases} |x|_q = 1 \text{ si } q \neq p_i \\ |x|_{p_i} = {p_i}^{-\alpha_i} \\ |x|_\infty = p_1^{\alpha_1} \dots p_k^{\alpha_k} \end{cases}$$

d'où le résultat

Proposition 10. *La distance d_p est ultramétrique. Ainsi une série à coefficent dans $\mathbb{Q}_p$ converge si et seulement si son terme général tend vers 0.*

Remarque 2.1. On observe que Q_p est le complété de $\mathbb{Q}$ pour la valeur absolue p-adique et $\mathbb{R}$ le complété de $\mathbb{Q}$ pour la valeur usuelle. Le théorème de Ostrowski assure que toute valeur absolue non triviale sur $\mathbb{Q}$ est équivalente à la valeur absolue archimédienne $|.|$ usuelle ou à une certaine valeur absolue p-adique $|.|_p$. On a donc tous les complétés de $\mathbb{Q}$.

Proposition 11. *$\mathbb{Q}$ est dense dans $\mathbb{Q}_p$*

Démonstration. C'est la propriété fondamental du complété !

Définition 11. *On définit l'ensemble $\mathbb{Z}_p := \{a \in \mathbb{Q}_p,\ v_p(a) \geq 0\}$*

Proposition 12. *$\mathbb{Z}_p$ est un sous-anneau de $\mathbb{Q}_p$. C'est l'anneau des **entiers p-adique**.*

2.2 Construction de $\mathbb{Z}_p$ et $\mathbb{Q}_p$: approche algébrique

Comme le titre de la section le suggère, nous allons construire cette-fois ci de manière algébrique le corps des entiers p-adique et montrer que les deux constructions sont en fait les mêmes.

2.2.1 Contruction de $\mathbb{Z}_p$

Définition 12.
Pour tout $n \geq 1$, on pose $A_n = \mathbb{Z}/p^n\mathbb{Z}$. On peut observer qu'un élément de A_n définit entièrement un élément de A_{n-1}. On a donc un morphisme $\Phi_n : A_n \to A_{n-1}$ qui est surjectif, et de noyau $p^{n-1}A_n$.
La suite $\dots \to A_n \to A_{n-1} \to \dots \to A_1$ constitue un "système projectif".

Définition 13. *On désigne par anneau des entiers p-adiques noté $\mathbb{Z}_p$, la limite du système projectif (A_n, Φ_n). Par définition un élement de $\mathbb{Z}_p$ est une suite $x = (\dots, x_n, \dots, x_1)$ avec $x_n \in A_n$ et $\Phi_n(x_n) = x_{n-1}$ si $n \geq 2$. On définit naturellement l'addition et la multiplication dans $\mathbb{Z}_p$ par l'addition et la multiplication coordonnées par coordonnées.*

Par exemple, 7 en tant que nombre 2-adique serait la suite $(1, 3, 7, 7, 7, 7, 7, \dots)$ écrit dans le sens inverse de la définition.

2.2.2 Lien entre $\mathbb{Z}_p^{topo}$ et $\mathbb{Z}_p^{alg}$

Définition 14. *On définit* $\mathbb{Z}_{(p)} := \{\frac{a}{b}, a, b \in \mathbb{Z},\ b \nmid p\}$. *C'est un sous-anneau de* $\mathbb{Q}$.

Proposition 13. *On a* $\mathbb{Z}_p^{topo} \simeq \mathbb{Z}_p^{alg}$.

Démonstration. La démonstration nécessite le lemme suivant :

Lemme 4. *1) Soit* $m \in \mathbb{N}$, *on a* $p^m\mathbb{Z}_p = \{a \in \mathbb{Q}_p | v_p(a) \geq m\}$

2) $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$. *Dans* $\mathbb{Q}_p$, $\mathbb{Q} \cap \mathbb{Z}_p = \mathbb{Z}_{(p)}$

3) $\forall m \in \mathbb{N}^*, \mathbb{Z}/p^m\mathbb{Z} \simeq \mathbb{Z}_{(p)}/p^m\mathbb{Z}_{(p)} \simeq \mathbb{Z}_p/p^m\mathbb{Z}_p$

2.2.3 Premières propriétés de $\mathbb{Z}_p$

Soit ϵ_n l'application n-ième composante.

Définition 15. *Une suite exacte de groupes abéliens peut être écrite comme suit :*

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

où les applications f *et* g *sont des homomorphismes de groupes tels que* $\mathrm{Im}(f) = \ker(g)$.

Proposition 14.
La suite $0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\epsilon_n} A_n \to 0$ *est exacte.*

Proposition 15. *On a les propriétés suivantes :*

i) Un élément de $\mathbb{Z}_p$ *(resp. de* A_n*) soit inversible, il faut et il suffit qu'il ne soit pas divisible par* p.

ii) Si U *désigne le groupe des éléments inversibles de* $\mathbb{Z}_p$, *tout élément de* $\mathbb{Z}_p$ *différent de* 0 *s'écrit de façon unique sous la forme* $p^n u$, *avec* $u \in U$ *et* $n \geq 0$.

Démonstration. i) On montre la propriété pour A_n en effet un élément est inversible si et seulement si chacune de ses composantes l'est. Soit $a \in A_n$ alors a est inversible si et seulement si a est premier avec p^n si et seulement si il est premier avec p.

ii) Existence : Soit $a \in \mathbb{Z}_p$ si a est non nul on note n le plus grand entier entier tel que la n-ième composante de a soit nul. On a donc $p^{-n}a$ n'est pas divisible par p donc est inversible. On note donc u cet élément et ceci fournit le résultat. Unicité : Soient $n, m \geq 0$ et $u, v, \in U$ tels que $a = p^n u = p^m v$. Quitte à échanger n et m on peut supposer que $n \geq m$ on a donc $p^{n-m} = vu^{-1}$ donc est inversible donc $n = m$ car sinon p diviserait p^{n-m}.

Proposition 16. *L'anneau $\mathbb{Z}_p$ est un **anneau de valuation**, de manière équivalente, c'est un anneau **principal** possédant pour **unique idéal maximal** $\mathfrak{m} := p\mathbb{Z}_p$. C'est donc un anneau **local**, dont les idéaux sont donnés par la chaîne $A \supsetneq \mathfrak{m} \supsetneq \mathfrak{m}^2 \supsetneq \mathfrak{m}^3 \supsetneq ....$ Les éléments irréductibles (/ premiers /extrémaux) sont les pu où $u \in U$.*

Démonstration. La valuation v sur $\mathbb{Z}_p$ (qui à tout $p^n u \in \mathbb{Z}_p$, avec $n \in \mathbb{N}$ et $u \in U$ associe n) s'étend à $\mathbb{Q}_p = Frac(\mathbb{Z}_p)$ (voir paragraphe suivant) et l'on a clairement $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid v(x) \geq 0\}$. Le reste découle des propriétés des anneaux à valuation discrète.

2.2.4 Le corps $\mathbb{Q}_p$

Définition 16. *On appelle corps des fractions des nombres p-adiques, et on note $\mathbb{Q}_p$, le corps des fractions de l'anneau $\mathbb{Z}_p$.*

$\mathbb{Q}_p$ est bien définie car $\mathbb{Z}_p$ est intègre car c'est un anneau à valuation discrète.

Définition 17. *Soit $a = \sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p$ on définit la **valuation** de a par :*

$$v(a) = \begin{cases} min(i \in \mathbb{N}, a_i \neq 0) & si\ a \neq 0 \\ \infty & sinon \end{cases}$$

On étend facilement cette notion à $\mathbb{Q}_p$

Définition 18. *On définit les ensembles :*

$$\mathcal{O} := \{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\}$$

$$\mathfrak{m} := \{x \in \mathbb{Q}_p \mid v_p(x) > 0\}$$

$$k := \mathcal{O}/\mathfrak{m}$$

Définition 19. *Construction équivalente de $\mathbb{Q}_p$: Soit p un nombre premier. On définit la valeur absolue p-adique comme l'application $|.|_p : \mathbb{Q} \mapsto \mathbb{R}+$ vérifiant $|0|_p = 0$, et $|n|_p = p^{-v_p(n)}$ si n est un rationnel non nul. on peut montrer qu'un élément x de $\mathbb{Q}_p$ peut s'écrire $x = \sum_{i=k}^{\infty} a_i p^i$ où $a_i \in \{0, 1, \ldots, p-1\}$ et $k \in \mathbb{Z}$ (la convergence est au sens de la valeur absolue p-adique)*

Proposition 17. *Calcul de l'opposé dans $\mathbb{Z}_p$: Soit $a = \sum_{i=0}^{\infty} a_i p^i$ on a,*
$-a = 1 + \sum_{i=0}^{\infty}(p - 1 - a_i)$.

2.3 Propriétés de $\mathbb{Q}_p$ et de $\mathbb{Z}_p$

2.3.1 Topologie de $\mathbb{Z}_p$

Proposition 18. *L'anneau topologique $\mathbb{Z}$ s'injecte dans $\mathbb{Z}_p$, et y est dense.*

Démonstration. En fait, mieux que $\mathbb{Z}$ (qui appartient bien à $\mathbb{Z}_p$, vu que tous ses éléments n vérifient $v_p(n) \geq 0$, et ce pour tout p premier), l'ensemble $\mathbb{N}$ est dense dans $\mathbb{Z}_p$: si $x = \sum_{i=0}^{\infty} a_i p^i$ où $a_i \in \{0, 1, \ldots, p-1\}$, alors la suite $(x_n)_{n\geq 0}$ définie par $x_n = \sum_{i=0}^{n} a_i p^i$ la différence des deux est

divisible par p^n, donc la valeur absolue p-adique de $x - x_n$ est majorée par p^{-n},qui tend vers 0 quand n tend vers l'infini.

Proposition 19. *$\mathbb{Z}_p$ est compact*

Démonstration. On a : $\mathbb{Z}_p$ est un fermé d'un produit de compacts (et même d'ensembles finis); il est donc compact d'après le théorème de Tykhonov.

2.4 Equations p-adique

En général, l'étude de zéros de fonctions ou de polynômes revient très souvent en mathématique. Le problème est que parfois on ne sait ni l'existence ni l'expression de ces zéros. Dans cette partie nous allons utiliser le lemme de Hensel outil très puissant, qui permet à partir d'une solution approchée de trouver une solution exacte.

2.4.1 Limites projectives et racines

Lemme 5. *Soit $\ldots \to X_n \to X_{n-1} \to \ldots \to X_1$ un système projectif et X sa limite projective. Si les X_n sont finis et non vides, X est non-vide.*

Notation : Si f est un polynôme à coefficients dans $\mathbb{Z}_p$, et si $n \geq 1$, on note f_n le polynôme à coefficients dans A_n déduit de f par réduction modulo p^n.

Proposition 20. *Soient $f^{(i)} \in [X_1, \ldots, X_m]$ des polynômes à coefficients entiers p-adiques. Les propositions suivantes sont équivalentes :*

i) Les $f^{(i)}$ ont un zéro commun dans ${\mathbb{Z}_p}^m$.

ii) Pour tout $n \geq 1$, les polynômes $(f_n)^{(i)}$ ont un zéro commun dans $(A_n)^m$.

Notation : Un point $x = (x_1, ..., x_m)$ de $(\mathbb{Z}_p)^m$ est dit "primitif" si l'un des x_i est inversible, c'est à dire si les x_i ne sont pas tous divisibles par p; on définit de manière analogue les éléments primitifs de $(A_n)^m$.

Proposition 21. *Soient $f^{(i)} \in \mathbb{Z}_p[X_1, ..., X_m]$ des polynômes homogènes à coefficientss entiers p-adiques. Il y a équivalence entre :*

a) Les $f^{(i)}$ ont un zéro commun non trivial dans $(\mathbb{Q}_p)^m$.

b) Les $f^{(i)}$ ont un zéro commun primitif dans $(\mathbb{Z}_p)^m$.

c) Pour tout $n \geq 1$, les $f_n^{(i)}$ ont un zéro commun primitif dans $(A_n)^m$.

2.4.2 Amélioration des solutions approchées

Lemme 6. *Lemme de Hensel : Soit $f \in \mathbb{Z}_p[X]$, et f' sa dérivée. Soient $x \in \mathbb{Z}_p$,$n, k \in \mathbb{Z}$ tels que $0 \leq 2k < n$, $f(x) \equiv 0 \pmod p$,$v_p(f'(x)) = k$. Il existe alors $y \in \mathbb{Z}_p$ tel que : $f(y) \equiv 0 \pmod{p^{n+1}}$, $v_p(f'(y)) = k$ et $y \equiv x \pmod{p^{n-k}}$.*

Démonstration. On considère y de la forme $x+p^{n-k}z$ avec $z \in \mathbb{Z}_p$. La formule de Taylor assure que :

$f(y) = f(x) + p^{n-k}zf'(x) + p^{2n-2k}a$ avec $a \in \mathbb{Z}_p$. D'après les hypothèses on a $f(x) = p^n b$ et $f'(x) = p^k c$, avec $b \in \mathbb{Z}_p$ et $c \in \mathbb{U}$; il est donc possible de prendre z tel que $b + cz \equiv 0 \pmod p$. La formule précédente permet donc d'avoir :
$f(y) = p^n(b + cz) + p^{2n-2k} \equiv 0 \pmod{p^{n+1}}$ car $2n - 2k > n$.
On réapplique la formule de Taylor cette fois-ci à f', on $f'(y) \equiv p^k c \pmod p$ or $n - k > k$ donc on a bien $v_p(f'(y)) = k$.

Théorème 3. *Soient $f \in \mathbb{Z}_p[X_1, ..., X_m]$, $x = (x_i) \in (\mathbb{Z}_p)^m$,$n, k \in \mathbb{Z}$, et $j \in [\![1 \ ; \ n]\!]$. On suppose que $0 \leq 2k < n$, et que $f(x) \equiv 0 \pmod{p^n}$ et $v_p(\frac{\partial f}{\partial X_j}(x)) = k$.*
Il existe un zéro y de f dans $(\mathbb{Z}_p)^m$ qui est congru à x modulo p^{n-k}.

Démonstration. On prouve d'abord le théorème pour $m = 1$. On applique le lemme précédent à $x^{(0)} = x$, on obtient $x^{(1)} \in \mathbb{Z}_p$, avec $x^{(1)} \equiv x^{(0)} \pmod{p^{n-k}}$ et tel que : $f(x^{(1)}) \equiv 0 \pmod{p^{n+1}}$, et $v_p(f'(x^{(1)})) = k$ On réapplique le lemme à $x^{(1)}$. Ainsi on construit une suite $x^{(0)}, x^{(1)}, \ldots, x^{(q)}, \ldots$ avec :
$x^{(q+1)} \equiv x^{(q)} \pmod{p^{n+q-k}}$ et $f(x^{(q)}) \equiv 0 \pmod{p^{n+q}}$. On peut remarquer que c'est une suite de Cauchy donc converge vers un certain y. On peut affirmer qu'alors : $f(y) = 0$ et $y \equiv x \pmod{p^{n-k}}$, ce qui conclut la preuve pour le cas $m = 1$.
Si $m > 1$ on peut se ramener au cas précédent en construisant le polynôme à une variable $\tilde{f} \in \mathbb{Z}_p[X_j]$ obtenu en remplaçant les X_i par x_i pour $i \neq j$.On applique le résultat précédent à $\tilde{f}$ et à x_j. On prouve ainsi l'existence de $y_j \equiv x_j \pmod{p^{n-k}}$ avec $\tilde{f}(y_j) = 0$. On pose $y_i = x_i$ pour $i \neq j$ et $y = (y_i)$ est solution.

2.4.3 Applications du lemme de Hensel

Une application directe du lemme de Hensel permet par exemple d'étudier les inversibles de $\mathbb{Z}_p$:

Proposition 22. *Inversibles de $\mathbb{Z}_p$*
Considérons le polynôme $P = aX - 1$, avec $a \in \mathbb{Z}_p \backslash p\mathbb{Z}_p$. P admet une racine approchée mod p car a_0 est non nul, donc inversible dans le corps F_p. De plus, $P'(x) = a$ et $v(a) = 0$ (a inversible), donc cette racine mod p peut être améliorée en une racine mod p^n pour $n \in \mathbb{N}$. Par le lemme de Hensel, il existe $\xi \in \mathbb{Z}_p$ tel que $P(\xi) = 0$, i.e. $a\xi = 1$. D'où l'inclusion $p\mathbb{Z}_p \subset \mathbb{Z}_p^*$. La réciproque est évidente.

Corollaire 1. *1. Tout zéro simple de la réduction modulo p d'un polynôme f se relève en un zéro de f à coefficients dans $\mathbb{Z}_p$. (On rappelle que si Q est un polynôme sur un corps, un zéro de Q est dit simple si au moins l'une des dérivées partielles $\frac{\partial Q}{\partial X_j}$ est nul en x.)*

Ou bien pour les zéros de formes quadratiques :

Corollaire 2. *Supposons que $p \neq 2$. Soit $f(X) = \sum a_{ij}X_iX_j$ avec $a_{ij} = a_{ji}$, une forme quadratique à coefficients dans $\mathbb{Z}_p$ dont le discriminant $det(a_{ij})$ est inversible. Soit $a \in \mathbb{Z}_p$. Toute solution primitive de l'équation $f(x) \equiv a \pmod p$ se relève en une solution exacte.*

3 Séries p-adiques ; logarithme et exponentielle p-adiques

Nous allons étudier les séries p-adique et leur comportement bien différent du cas réel ou complexe.

3.1 Séries p-adique

3.1.1 Propriétés

Proposition 23. *Une série p-adique converge si, et seulement si son terme général tend vers 0.*

Démonstration. Le sens direct est évident. La réciproque est vrai car $(\mathbb{Q}_p, |.|_p)$ est un espace ultramétrique. Une série de terme général (u_n) converge si, et seulement si elle vérifie le critère de Cauchy, car $\mathbb{Q}_p$ est complet. Or on a $\left(\sum_{k=n}^{n+m} u_k\right)_p \leq \max_{k\in[\![n,n+m]\!]} |u_k|_p$. Soit $\varepsilon > 0$. Si la suite $(u_n)_{n\geq 0}$ tend vers 0, alors pour n assez grand, on a $|u_n|_p < \varepsilon$. Toujours pour ce n très grand, et indépendamment de m, on a $\sum_{k=n}^{n+m} u_k)_p < \varepsilon$, donc la série vérifie le critère de Cauchy, et converge.

Exemple : La série de terme général p^n converge car son terme général tend vers 0. Sa somme vaut $\sum_{n=0}^{\infty} p^n = \frac{1}{1-p}$. Ceci diffère du cas réel où la raison doit être de module strictement plus petit que 1.

Théorème 4. *Soit une série $\sum a_n$ avec $a_n \in \mathbb{Q}_p$ pour tout n. Alors la série est convergente si et seulement si $\lim_{n\to\infty} a_n = 0$. Dans ce cas $|\sum_{n+0}^{\infty} a_n| \leq max_n(a_n)$*

Définition 20. *De manière analogue dans $\mathbb{C}$ ou $\mathbb{R}$ on peut aussi définir le rayon de convergence d'une série entière. On considère $f = \sum_{n=0}^{\infty} a_nX^n \in \mathbb{Q}_p[[X]]$ une série formelle. On appelle rayon de convergence de f, et on note R_f, la borne supérieure de l'ensemble : $\{r \in \mathbb{R}^+; |a_n|_p r^n \to 0\}$.*
On a donc : $\forall x \in \mathbb{Q}_p$ tel que $|x|_p > R_f$, la série $\sum_{n\geq 0} a_nx^n$ converge.

Proposition 24. *Soit $f(X) = \sum_{n=0}^{\infty} a_nX^n$ et soit*

$$\rho = \frac{1}{\limsup_{n\to\infty} |a_n|_p^{1/n}}$$

. On a :

- *Si $\rho = 0$, la série converge seulement en 0*
- *Si $\rho = +\infty$ la série converge sur $\mathbb{Q}_p$ tout entier.*
- *Si $0 < \rho < \infty$ et $\lim_{n\to\infty} |a_n|\rho^n = 0$, la série $f(x)$ converge si et seulement si $|x|_p \leq \rho$.*
- *Si $0 < \rho < \infty$ et $\lim_{n\to\infty} |a_n|\rho^n \neq 0$, la série $f(x)$ converge si et seulement si $|x|_p < \rho$.*

Démonstration. D'après la proposition 26, on sait que le domaine de convergence est $\{x \in \mathbb{Q}_p, \lim_{n\to\infty} |a_n x^n|_p = 0\}$. Si $x < \rho$, on peut remarquer que la série $\sum |a_n|_p |x|_p^n$ est convergente donc la série p-adique converge. Dans le cas $|x| > \rho$, la série de terme générale $|a_n||x|_p^n$ diverge grossièrement, en effet par définition de la limite sup, on aurait pour une infinité de n $|a_n|_p$ proche de $\frac{1}{p^n}$ or comme $|x|_p > \rho$, $(\frac{|x|}{\rho}^n)$ devient de plus en plus grand. Puis le cas $|x|_p = \rho$ est une conséquence direct de la proposition 26.

Proposition 25. *Soit $a_{ij}\mathbb{Q}_p$ une famille de nombres p-adiques tels que $\forall \epsilon > 0$, il existe $N = N(\epsilon)$ tel que $max_{i,j} \geq N \implies |b_{i,j}|_p < \epsilon$. Alors les deux séries $\sum_i(\sum_j b_{ij})$ et $\sum_j(\sum_i b_{ij})$ sont convergentes et leurs sommes sont égales.*

Dans le cas complexe, le comportement au bord du disque ouvert de convergence n'est pas connu. Dans les corps p-adique la situation est plus facile :

Proposition 26. *Le domaine de convergence d'une série entière p-adique $f \in \mathbb{Q}_p[[X]]$ est une boule fermée $\overline{B_f}(0, R)$, où R est soit un p^k pour un k entier, soit dans l'ensemble $\{0, \infty\}$.*

Lemme 7. *Soit $f(X) = \sum a_n X^n$ une série entière à coefficients dans $\mathbb{Q}_p$, si on note $\mathcal{D} \subset \mathbb{Q}_p$ son domaine de convergence. Alors l'application :*

$$\mathcal{D} \to \mathbb{Q}_p, x \mapsto f(x) \text{ est continue}$$

Démonstration. Soit $x \in \mathcal{D}$ et $\epsilon > 0$. Montrons qu'il existe $\delta > 0$ tel que $\forall y \in \mathcal{D} \cap B(x, \delta) \implies |f(y) - f(x)|_p < \epsilon$. On a $|f(y) - f(x)|_p = |\sum_{n=0}^{\infty} a_n(y^n - x^n)|_p$. Or la série converge normalement donc uniformément sur $\mathcal{D}$ donc il existe un entier N tel que le N-ième reste partiel soit plus petit que $\frac{\epsilon}{2}$. Puis par continuité des polynômes sur $\mathbb{Q}_p$ il existe $\delta > 0$ tel que $y \in B(x, \delta)$ $|\sum_{n=0}^{N} a_n(y^n - x^n)|_p < \epsilon/2$. Ainsi $|f(y) - f(x)|_p \leq \max(|\sum_{n=0}^{N} a_n(y^n - x^n)|_p, |\sum_{n=N+1}^{\infty} a_n(y^n - x^n)|_p) < \epsilon/2 < \epsilon$.

Théorème 5. *Théorème de Strassman : Soit $f(X) = \sum_{n=0}^{\infty} a_n X^n$ une série entière à coefficients dans $\mathbb{Q}_p$ non-nulle. On suppose que $\lim_{n\to\infty} a_n = 0$, ainsi $f(x)$ converge pour tout $x \in \mathbb{Z}_p$. Soit $N \in \mathbb{N}$ défini par $|a_N|_p = max_n(|a_n|_p)$ et $|a_n|_p < |a_N|_p$ pour $n > N$. Alors la fonction $f : \mathbb{Z}_p \to \mathbb{Q}_p, x \mapsto f(x)$ a **au plus N zéros**.*

Démonstration. L'existence de l'entier N est assurée par le fait que $\lim_{n\to\infty} a_n = 0$. Il existe une valeur maximale de la norme d'un coefficient et N représente le rang de ce dernier coefficient où le maximum est atteint. On raisonne par récurrence sur N.

Si $N = 0$: Soit $x \in \mathbb{Z}_p$ tel que $f(x) = 0$. On a donc $|a_0|_p = |a_1 x + a_2 x^2 + \dots|_p \leq \max_{n\geq 1}(|a_n x^n|_p) \leq \max_{n\geq 1}(|a_n|)_p$ ce qui est absurde par définition de N.

Héridité : On suppose que $|a_N|_p = \max_n(|a_n|_p)$ et $|a_n|_p < |a_N|_p$ pour $n > N$. Soit $\alpha \in \mathbb{Z}_p$ tel que $f(\alpha) = 0$. Soit $x \in \mathbb{Z}_p$ quelconque, on a : $f(x) = f(x) - f(\alpha) = (x - \alpha)\sum_{n\geq 1}\sum_{j<n} a_n x^j \alpha^{n-1-j}$ d'après la proposition 28 on peut réarranger les sommes. On obtient $f(x) = (x - \alpha)\sum_{n=0}^{\infty} b_n x^n$ avec $b_n = \sum_{k\geq 0} a_{n+1+k}\alpha^k$. On observe que : $|b_j|_p \leq \max_{k\geq 0}|a_{j+k+1} \leq |a_N|_p$ et $|b_{N-1}|_p = |a_N + a_{N+1}\alpha + \dots|_p = |a_N|$. Et pour $j \geq N$, on a $|b_j|_p \leq \max_{j\geq N+1}|a_{j+k+1}|_p \leq \max_{j\geq N+1}|a_j| < |a_N|_p$. On peut donc appliquer l'hypothèse de récurrence à la série entière $g(x) = \sum_{n\geq 1}\sum_{j<n} a_n x^j \alpha^{n-1-j}$. On en déduit que f a au plus $N + 1$ zéros les N zéros de g et α.

Corollaire 3. *Soit $f(X) = \sum_{n=0}^{\infty} a_n X^n$ une série entière à coefficients dans $\mathbb{Q}_p$ qui converge sur $\mathbb{Z}_p$ et soit $\alpha_1, \dots, \alpha_m$ les racines de f dans $\mathbb{Z}_p$. On peut trouver une série entière g qui converge sur $\mathbb{Z}_p$ mais n'ayant aucun entier p-adique comme zéro et telle que*

$$f(X) = (X - \alpha_1) \dots (X - \alpha_m) g(X)$$

Démonstration. Clair d'après la construction de la démonstration du théorème.
On en déduit le corollaire suivant en "rescalant" la variable :

Corollaire 4. *Soit $f(X) = \sum_{n=0}^{\infty} a_n X^n$ une série entière à coefficients dans $\mathbb{Q}_p$ qui converge sur $p^m\mathbb{Z}_p$ pour un certain $m \in \mathbb{Z}$. Alors $f(X)$ a un nombre fini de zéros dans $p^m\mathbb{Z}_p$.*

3.1.2 Quelques résultats sur des séries p-adiques classiques

Proposition 27. *La série entière $\sum_{n\geq 0} \frac{t^n}{n!}$ converge sur $B\left(0, p^{\frac{-1}{p-1}}\right)$*

Remarque 3.1. On observe que le rayon de convergence de la série exponentielle n'est pas $+\infty$ comme dans le cas réel.

Démonstration. Soit n un entier ≥ 1 et p un nombre premier. Montrons que $v_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rceil$. Le nombre d'entier compris entre 1 et n divisible par p^k est exactement $\lfloor \frac{n}{p^k} \rceil$. En effet on a :

$|\{l \in [\![1, n]\!], p^k | l\}| = |\{l \in [\![1, n]\!], \exists i \in \mathbb{N}, l = p^k i\}| = |\{l \in [\![1, n]\!], \exists i \in \mathbb{N}, i = \frac{l}{p^k}\}| = \lfloor \frac{n}{p^k} \rceil$. On obtient le résultat souhaité en utilisant le fait que $v_p(ab) = v_p(a) + v_p(b), a, b \in \mathbb{N}$. On en déduit que $v_p(p^m!) = p^{m-1} + p^{m-2} + \dots + 1$. On considère désormais la décomposition de n en base p i.e $n = a_0 + a_1 p + a_2 p^2 + \dots + a_s p^s$ avec $0 \leq a_j \leq p - 1$. Si on pose $S_n = \sum_j a_j$ on a $v_p(n!) = \frac{n - S_n}{p-1}$. En effet on utilise le premier résultat : $v_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rceil$ or on a $\lfloor \frac{n}{p} \rceil = \frac{n - a_0}{p}$, $\lfloor \frac{n}{p^2} \rceil = \frac{n - a_0 - a_1 p}{p^2}$ et ainsi de suite, en factorisant on obtient bien le résultat.

Si $|t|_p < p^{-1/(p-1)}$, alors : $\left|\frac{t^n}{n!}\right|_p = p^{-n\, v_p(t)} / |n!|_p < p^{-n\left(v_p(t) + \frac{1}{p-1}\right)} \to 0$ car $v_p(n!) > \frac{n}{p-1}$ d'après le travail précédent.

Proposition 28. *Soit $x \in \mathbb{Q}$, on a $\lim_{i\to\infty} \frac{|x_i|}{i!}_p = 0$ si et seulement si $v_p(x) \geq 1$ si $p \neq 2$, $v_2(x) \geq 2$ si $p = 2$.*

Démonstration. C'est la preuve de la proposition précédente.

Proposition 29. *On peut définir aussi le logarithme p-adique : la série entière $\sum_{n\geq 0} (-1)^{n+1} \frac{t^n}{n}$ converge sur $B(0, 1)$.*

Démonstration. En effet, $\frac{1}{n} \to 0$ et $\lim_{n\to\infty} |a_n|_p^{1/n} = 1$.

On retrouve les propriétés de l'exponentielle et du logarithme :

Proposition 30. *1) Si x_1 et x_2 appartiennent au domaine de convergence de la série exponentielle on a :* $\exp(x_1 + x_2) = \exp(x_1)\exp(x_2)$.

2) Si t_1 et t_2 appartiennent au domaine de convergence de la série logarithme on a : $\log(t_1 t_2) = \log(t_1) + \log(t_2)$.
3) Dans les bons domaines, on a $\exp(\log(x)) = x = \log(\exp(x))$

4) Soit $m \geq 1$ si $p \neq 2$ et $m \geq 2$ si $p = 2$. Alors exp *et* log *sont des isomorphismes réciproques l'un de l'autre : $p^m\mathbb{Z}_p \simeq 1 + p^m\mathbb{Z}_p$ avec $p^m\mathbb{Z}_p$ vu comme groupe additif et $1 + p^m\mathbb{Z}_p$ comme groupe multiplicatif.*

Proposition 31. *1) Tout élément de $\mathbb{Q}_p^\times$ s'écrit de manière unique $p^n u$ avec $n \in \mathbb{Z}, u \in \mathbb{Z}_p^\times$. Ainsi $\mathbb{Z} \times \mathbb{Z}_p^\times \xrightarrow{\simeq} \mathbb{Q}_p^\times; (n, u) \to p^n u$.*

2) Soit $G = \{x \in \mathbb{Z}_p^\times | x^{p-1} = 1\}$ et soit l'homomorphisme de groupe $\mathbb{Z}_p^\times \to \mathbb{F}_p^\times$ induit par l'application réduction modulo p dans $\mathbb{Z}_p$. On a $G \to \mathbb{Z}_p^\times \to \mathbb{F}_p^\times$ est une bijection et $\mathbb{Z}_p^\times$ est le produit direct de G et de $1 + p\mathbb{Z}_p$.

3) Si $p \neq 2$ le groupe multiplicatif $1 + p\mathbb{Z}_p$ est isomorphe à $\mathbb{Z}_p$. Dans le cas $p = 2$, $1 + 2\mathbb{Z}_2$ est le produit direct de $\{\pm 1\}$ et $1 + 4\mathbb{Z}_2$.

Démonstration. 1) Clair. Si $p \neq 2$ le point 3) découle du fait que $1 + p\mathbb{Z}_p \simeq p\mathbb{Z}_p$ grâce à exp et log et $\mathbb{Z}_p \xrightarrow{\simeq} p\mathbb{Z}_p$ via l'isomorphisme $a \mapsto pa$. De même pour le cas $p = 2$ on a $1 + 4\mathbb{Z}_2 \xrightarrow{\simeq} 4\mathbb{Z}_2$. Prouvons désormais 2). On peut remarquer que le noyau de l'application $\mathbb{Z}_p^\times \to \mathbb{F}_p^\times$ $x \to \overline{\epsilon_0(x))}$ est $1 + p\mathbb{Z}_p$. On peut se contenter de prouver que $G \to \mathbb{F}_p^\times$ est une bijection. Pour l'injectivité nous avons besoin de prouver que $G \cap (1 + p\mathbb{Z}_p) = \{1\}$. Si $p = 2$ c'est trivial car $G = \{1\}$. Si $p \neq 2$, on a $1 + p\mathbb{Z}_p \simeq \mathbb{Z}_p$ n'a comme élément d'ordre fini que l'unité donc l'intersection est réduite à l'unité. Pour le caractère surjectif, si $p = 2$ c'est trivial car $\mathbb{F}_2^\times = \{1\}$. Pour $p \neq 2$, soit $a \in \mathbb{F}_p^\times$ et $u \in \mathbb{Z}_p$ tel que son image dans $\mathbb{F}_p$ soit a. Par hypothèse $a^{p-1} = 1$ donc $u^{p-1} \in 1 + p\mathbb{Z}_p$. Soit

$$v = \exp(\frac{1}{p-1}\log(u^{p-1}))$$

qui est bien défini et $w = uv^{-1}$. On a $w \in G$ car $v^{p-1} = u^{p-1}$ d'après les proprités de l'exponentielle et du logarithme. Comme $v \in 1 + p\mathbb{Z}_p$ l'image de w dans $\mathbb{F}_p^\times$ est a. De plus $u = wv$, ce qui prouve le produit direct.su

3.1.3 Inversibles de $\mathbb{Q}_p$

Proposition 32. *Si $p \neq 2$, on a $\mathbb{Q}_p^\times \simeq \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$.*
Si $p = 2$, on a $\mathbb{Q}_2^\times \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$.

Démonstration. Pour $p \neq 2$, d'après la proposition précédente on a : $\mathbb{Q}_p^\times \simeq \mathbb{Z} \times \mathbb{Z}_p^\times \simeq \mathbb{Z} \times G \times (1 + p\mathbb{Z}_p) \simeq \mathbb{Z} \times \mathbb{F}_p^\times \times (1 + p\mathbb{Z}_p) \simeq \mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$. Idem pour le cas $p = 2$. De même dans le cas $p = 2$ il faut cette fois-ci remplacer 2 par 4.

3.1.4 Carrés de $\mathbb{Q}_p$

Proposition 33. *Soit $a = p^n u \in \mathbb{Q}_p^\times$ $(n \in \mathbb{Z}, u \in \mathbb{Z}_p^\times)$ alors a est un carré dans $\mathbb{Q}_p^\times$ si et seulement si* $\begin{cases} n \text{ pair} \\ \text{si } p \neq 2,\ u \mod p\mathbb{Z}_p \text{ est un carré dans } \mathbb{F}_p^\times, \text{ si } p = 2, u \equiv 1 \mod 8\mathbb{Z}_2 \end{cases}$

Démonstration. D'après le point 1) de la proposition 27), a est un carré si et seulement si n est pair et u est un carré de $\mathbb{Z}_p^\times$. Dans le cas $p \neq 2$, $1 + p\mathbb{Z}_p = \exp(\mathbb{Z}_p) = \exp(2p\mathbb{Z}_p) = \{\exp(p\mathbb{Z}_p)\}^2$, ainsi un élement de $1 + p\mathbb{Z}_p$ est un carré dans $\mathbb{Z}_p^\times$. De plus $\mathbb{Z}_p^\times/(1 + p\mathbb{Z}_p) \simeq \mathbb{F}_p^\times$ d'où le résultat.

4 Théorème de Skolem-Mahler

Dans cette section, nous allons démontrer le but de cet écrit : le théorème de Skolem-Mahler grâce à l'aide de l'analyse p-adique.

Théorème 6. *Soit $(u_n)_{(n\in\mathbb{N})}$ une suite récurrente linéaire entière. Alors en notant $S = \{n \in \mathbb{N} | u_n = 0\}$ alors S est de la forme $\{ensemble finie\} \cup \{réunion\ finie\ de\ suite\ arithmétique\}$.*

Démonstration. Soit $(u_n)_{n\geq 0}$ une suite vérifiant la relation de récurrence linéaire :

$$\forall n \geq d,\ u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_d u_{n-d}$$

avec a_d non nul. Alors, on peut écrire

$$u_n = X^T A^n Y = \langle A^n X, Y\rangle,$$

où X et Y sont des vecteurs colonnes de longueur d, et A une matrice inversible de taille $d \times d$, qui dépendent des a_i et $u_0, \ldots, u_{d-1}$, et sont donc à coefficients entiers ; il n'est pas nécessaire de décrire précisément les coefficients des vecteurs et matrices. Comme A est inversible, son déterminant est non nul. Soit p un nombre premier qui ne divise pas ce déterminant. Alors A est inversible modulo p, et les matrices $A^n \mod p$ le sont également. Comme l'ensemble $\mathrm{M}_d(\mathbb{Z}/p\mathbb{Z})$ est fini (de cardinal p^{d^2}), il existe deux entiers n et m, avec $n < m$, tels que $A^n \equiv A^m \mod p$, puis $A^{m-n} \equiv \mathrm{Id} \mod p$, où Id est la matrice identité. Notons $M = m - n > 0$.
Alors, pour tout $r \in \{0, 1, \ldots, M-1\}$, l'ensemble :

$$\{n \in \mathbb{N};\ u_{Mn+r} = 0\}$$

est soit fini, soit égal à tout $\mathbb{N}$; ceci impliquerait le théorème de Skolem-Mahler-Lech (car les progressions arithmétiques $r + M\mathbb{Z}$ partitionnent $\mathbb{Z}$ quand r varie). Pour le prouver, supposons qu'il ne soit pas fini pour un certain r. Alors, $\langle A^{Mn} A^r X, Y\rangle = 0$ pour une infinité de valeurs de n. Par construction de M, on peut écrire :

$$A^M = \mathrm{Id} + pB$$

pour une certaine matrice B à coefficients entiers. Alors, $P(n) = 0$ pour une infinité d'entiers n, où P est défini sur $\mathbb{Z}$ par la formule :

$$P(n) = \langle (\mathrm{Id} + pB)^n A^r X, Y\rangle.$$

Développons l'expression $(\mathrm{Id} + pB)^n$ à l'aide du binôme de Newton, on trouve que $P(n)$ se met sous la forme d'une série formelle en p, dont les coefficients dépendent de n :

$$P(n) = \sum_{j=0}^{\infty} p^j P_j(n).$$

Chaque polynôme P_j est un polynôme en n (ils dépendent d'un coefficient binomial $\binom{n}{k}$) à coefficients entiers (donc entiers p-adiques). Or, P est limite uniforme, pour la topologie p-adique, des $\sum_{j=0}^{N} p^j P_j(n)$: on a

$$\left| P(n) - \sum_{j=0}^{N} p^j P_j(n) \right|_p \leq p^{-N} \to 0,$$

qui ne dépendent pas de n. P est limite uniforme de polynômes de $\mathbb{Z}_p[X]$, on peut donc étendre continûment P en une fonction de $\mathbb{Z}_p$ dans $\mathbb{Z}_p$. Ainsi l'extension de P à $\mathbb{Z}_p$ est analytique donc d'après le corollaire 4, P=0 car admet une infinité de zéros dans $\mathbb{Z}_p$ ainsi l'ensemble $\{n \in \mathbb{N};\ u_{Mn+r} = 0\}$ est $\mathbb{N}$.

L'objectif du stage n'est pas de se borner à l'énoncé de ce dernier mais d'élargir sa culture mathématique. Nous allons donc porter notre attention sur la théorie de Galois, point essentiel de la théorie des nombres.

5 Théorie de Galois

Dans cette partie nous nous intéresserons à la théorie de Galois, prouverons certains résultats.

5.1 Extension de corps

5.1.1 Extensions, algébricité et transcendance

Définition 21. *Si $\mathbb{K}$ est un sous-corps de l'anneau $\mathbb{A}$, $\mathbb{A}$ est naturellement muni d'une structure de $\mathbb{K}-$algèbre. . Si $\mathbb{L}$ est un surcorps de $\mathbb{K}$, on dit que que muni de sa structure de $\mathbb{K}$-algèbre est une extension de $\mathbb{K}$ et on parle de l'extension (de corps) $\mathbb{L}/\mathbb{K}$. L'extension $\mathbb{L}/\mathbb{K}$ est finie si $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel de dimension finie ; cette dimension, notée $[\mathbb{L} : \mathbb{K}]$, est le degré de l'extension.*

Remarque 5.1. Par exemple, $\mathbb{C}/\mathbb{R}$ est une extension de degré 2, mais $\mathbb{R}/\mathbb{Q}$ n'est pas une extension finie (car sinon $\mathbb{R}$ serait dénombrable). Les extensions finies de $\mathbb{Q}$ sont appelées "corps de nombres".

Proposition 34. *Soit $\mathbb{K}$ un corps fini. Alors il existe $p \in \mathcal{P}$ et $d \in \mathbb{N}$ tels que $|\mathbb{K}| = p^d$.*

Voici un théorème fondamental dans l'étude des extensions de corps :

Théorème 7. *Théorème de la base télescopique : . Soient $\mathbb{L}/\mathbb{K}$ une extension de corps, V un $\mathbb{L}$-espace vectoriel, $(\lambda_i)_{i\in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, $(v_j)_{j\in J}$ une base de V sur $\mathbb{L}$.*
(i) La famille $(\lambda_i v_j)_{(i,j)\in I\times J}$ est une base de V sur $\mathbb{K}$.
(ii) Supposons V non nul. Alors le $\mathbb{K}$-espace V est de dimension finie si et seulement si l'extension $\mathbb{L}/\mathbb{K}$ est finie et le $\mathbb{L}$-espace V est de dimension finie. On a alors :

$$dim_{\mathbb{K}}(V) = [\mathbb{L} : \mathbb{K}] \times dim_{\mathbb{L}}(V)$$

Corollaire 5.
Soient $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$ deux extensions de corps, $(e_i)_{i\in I}$ une base de $\mathbb{L}$ sur $\mathbb{K}$, et $(f_j)_{j\in J}$ une base de $\mathbb{M}$ sur $\mathbb{L}$.

(i) La famille $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ sur $\mathbb{K}$.

(ii) L'extension $\mathbb{M}/\mathbb{K}$ est finie si et seulement si $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$ le sont aussi. Dans ce cas, on a :

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}] \times [\mathbb{L} : \mathbb{K}].$$

Ce corollaire affirme la transitivité des extensions finies. La formule donnant $[M : K]$ est la propriété de multiplicativité des degrés.

Définition 22. *Adjonction : Si E est une partie non vide de la $\mathbb{K}$-algèbre $\mathbb{A}$, on note $\mathbb{K}[E]$ **la plus petite $\mathbb{K}$-sous-algèbre de $\mathbb{A}$ contenant** E. On dit que $\mathbb{K}[E]$ est la sous-algèbre de $\mathbb{A}$ obtenue par adjonction à $\mathbb{K}$ des éléments de E. Si $E = \{x_1, \dots, x_m\}$ est fini, on note $\mathbb{K}[E] = \mathbb{K}[x_1, \dots, x_m]$. On a :*

$$\mathbb{K}[x_1, \dots, x_m] = \{P(x_1, \dots, x_m) \mid P \in \mathbb{K}[X_1, \dots, X_m]\}.$$

En particulier, pour $x \in \mathbb{A}$:

$$\mathbb{K}[\{x\}] = \mathbb{K}[x] = \{P(x) \mid P \in \mathbb{K}[X]\}.$$

Une $\mathbb{K}$-algèbre de la forme $\mathbb{A} = \mathbb{K}[x]$ est dite monogène.

Définition 23. *Si $\mathbb{L}$ est un surcorps de $\mathbb{K}$ et E une partie de $\mathbb{L}$, on note $\mathbb{K}(E)$ **le plus petit sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et** E. Si $E = \{x_1, \dots, x_m\}$ est fini, on a :*

$$\mathbb{K}(E) = \left\{ \frac{P(x_1, \dots, x_m)}{Q(x_1, \dots, x_m)} \ ; \ (P, Q) \in \mathbb{K}[X_1, \dots, X_m]^2, \ Q(x_1, \dots, x_m) \neq 0 \right\}$$

et on note

$$\mathbb{K}(E) = \mathbb{K}(x_1, \dots, x_m).$$

En particulier, pour x dans L :

$$\mathbb{K}(\{x\}) = \mathbb{K}(x) = \left\{ \frac{P(x)}{Q(x)} \ ; \ (P, Q) \in \mathbb{K}[X]^2, \ Q(x) \neq 0 \right\}.$$

Définition 24. *Soient A une $\mathbb{K}$-algèbre, x un élément de $\mathbb{A}$. Soit δ_x le morphisme de $\mathbb{K}$-algèbres :*
$\delta_x : \mathbb{K}[X] \to \mathbb{A}$, $P \mapsto P(x)$ On observe que l'image de δ_x est exactement $\mathbb{K}[x]$.

*Le noyau de δ_x est l'idéal annulateur de x. S'il est réduit à $\{0\}$, c'est-à-dire s'il n'existe aucun de polynôme non nul P de $\mathbb{K}[X]$ tel que $P(x) = 0$, x est dit **transcendant sur** $\mathbb{K}$. Dans ce cas, δ_x est un isomorphisme de $\mathbb{K}$-algèbres de $\mathbb{K}[X]$ sur $\mathbb{K}[x]$.*

*Sinon, x est dit **algébrique sur** $\mathbb{K}$. L'idéal annulateur de x est engendré par un unique polynôme unitaire de $\mathbb{K}[X]$, appelé polynôme minimal de x sur $\mathbb{K}$ et noté $\Pi_{K,x}$. Le degré de ce polynôme est appelé degré de x sur $\mathbb{K}$. Les annulateurs de x dans $\mathbb{K}[X]$ sont donc les multiples de $\Pi_{K,x}$ dans $\mathbb{K}[X]$.*

Remarque 5.2. Par exemple $\sqrt{2}$ est algébrique sur $\mathbb{Z}$ car racine du polynôme $X^2 - 2 \in \mathbb{Z}[X]$. Les réels e π sont transcendants, ce résultat a été prouvé par Hermite-Lindemann (1882).

Une propriété essentielle à retenir est : **algébricité = finitude**.

Proposition 35. *Soient $\mathbb{A}$ une $\mathbb{K}$-algèbre, $x \in \mathbb{A}$.*

(i) Si x est transcendant sur $\mathbb{K}$, alors $(x^i)_{i\in\mathbb{N}}$ est une $\mathbb{K}$-base de $\mathbb{K}[x]$. En particulier, $\mathbb{K}[x]$ est de dimension infinie sur $\mathbb{K}$.

(ii) Si x est algébrique de degré n sur $\mathbb{K}$, alors $(x^i)_{0\leq i\leq n-1}$ est une $\mathbb{K}$-base de $\mathbb{K}[x]$. En particulier, $\mathbb{K}[x]$ est de dimension n sur $\mathbb{K}$.

Corollaire 6. *Si $\mathbb{A}$ est une $\mathbb{K}$-algèbre de dimension finie, tout élément de $\mathbb{A}$ est algébrique sur $\mathbb{K}$.*

Proposition 36. *Soient $\mathbb{A}$ une $\mathbb{K}$-algèbre , $P \in \mathbb{K}[X]$ irréductible unitaire, $x \in A$ annulé par P. Nécessairement :*

$$\Pi_{\mathbb{K},x} = P.$$

Proposition 37. *Soient $\mathbb{A}$ une $\mathbb{K}$-algèbre **intègre** , $x \in \mathbb{A}$ algébrique sur $\mathbb{K}$ alors $\Pi_{K,x}$ est irréductible sur $\mathbb{K}[X]$.*

Décrivons désormais les éléments irréductibles d'une algèbre monogène.

Proposition 38. *Soient $\mathbb{A}$ une $\mathbb{K}$-algèbre, $x \in \mathbb{A}$.*

(i) Si x est transcendant sur $\mathbb{K}$, les inversibles de $\mathbb{K}[x]$ sont les scalaires non nuls.

(ii) Si x est algébrique sur $\mathbb{K}$ et si $P \in \mathbb{K}[X]$, l'élément $P(x)$ de $\mathbb{K}[x]$ est inversible dans $\mathbb{K}[x]$ si et seulement si $pgcd(P, \Pi_{\mathbb{K},x}) = 1$.

(iii) En particulier, $\mathbb{K}[x]$ est un corps si et seulement si x est algébrique sur $\mathbb{K}$ et $\Pi_{\mathbb{K},x}$ irréductible sur $\mathbb{K}$.

Une propriété essentielle à retenir est : **algébricité = finitude**. Le corollaire suivant nous fournit une équivalence entre ces deux notions.

Corollaire 7. *Soient $\mathbb{L}/\mathbb{K}$ une extension de corps, $x \in \mathbb{L}$. Il y a équivalence entre :*

(i) l'élément x est algébrique sur $\mathbb{K}$;

(ii) la $\mathbb{K}$-algèbre $\mathbb{K}[x]$ est un corps, i.e. $\mathbb{K}[x] = \mathbb{K}(x)$;

(iii) la $\mathbb{K}$-algèbre $\mathbb{K}[x]$ est de dimension finie ;

(iv) il existe une $\mathbb{K}$-sous-algèbre de $\mathbb{L}$ de dimension finie sur $\mathbb{K}$ et contenant x.

Proposition 39. *Soient x et y deux éléments de $\mathbb{L}$ algébriques sur K, de degrés respectifs m et n. Alors $\mathbb{K}(x,y)/\mathbb{K}$ est de degré fini majoré par mn. En particulier, $x+y$ et xy sont algébriques sur $\mathbb{K}$ de degré d'algébricité majoré par mn.*

Démonstration. On a $\Pi_{\mathbb{K}(x),y} | \Pi_{\mathbb{K},y}$ donc y est de degré au plus n sur $\mathbb{K}(x)$. La transitivité des extensions finis et multiplicativité des degrés prouve le premier point. Le second point se déduit du premier grâce aux inclusions $\mathbb{K}(x+y) \subset \mathbb{K}(x,y), \mathbb{K}(xy) \subset \mathbb{K}(x,y)$. On a le diagramme :

$$\begin{array}{ccc} \mathbb{K} & \xrightarrow{\quad m \quad} & \mathbb{K}(x) \\ {\scriptstyle n}\downarrow & & \downarrow{\scriptstyle n' \leq n} \\ \mathbb{K}(y) & \xrightarrow[m' \leq m]{} & \mathbb{K}(x,y) \end{array}$$

$$\mathbb{K} \longrightarrow \mathbb{K}(x+y) \longrightarrow \mathbb{K}(x,y)$$

$$\mathbb{K} \longrightarrow \mathbb{K}(xy) \longrightarrow \mathbb{K}(x,y)$$

Théorème 8. *L'ensemble des éléments de $\mathbb{L}$ algébriques sur $\mathbb{K}$ est un sous-corps de $\mathbb{L}$.*

Démonstration. D'après la proposition précédente il suffit de prouver que si $x \in \mathbb{L}^*$ alors $\frac{1}{x}$ est algébrique. Ce est vrai car x est algébrique de degré n sur $\mathbb{K}$, $X^n \Pi_{\mathbb{K},x}(1/X)$ annule $\frac{1}{x}$.

Proposition 40. *Les deux assertions suivantes sont équivalentes :*

(i) L'extension $\mathbb{L}/\mathbb{K}$ est finie.

(ii) Il existe $n \in \mathbb{N}$ et des éléments $x_1, ..., x_n$ de $\mathbb{L}$ algébriques sur $\mathbb{K}$ tels que $\mathbb{L} = \mathbb{K}(x_1, ..., x_n)$.

Démonstration. Pour *i)* $\implies$ *ii)* on prend pour $x_1, \ldots, x_n$ une base de $\mathbb{L}$ sur $\mathbb{K}$. Pour *ii)* $\implies$ *i)*, on raisonne par récurrence sur le degré de l'extension. Le cas $n = 1$ est trivial.
$n \implies n+1$: Soit Ω une extension de $\mathbb{K}$, $x_1, \ldots x_{n+1} \in \Omega$ algébriques sur $\mathbb{K}$ et $\mathbb{L} = \mathbb{K}(x_1, \ldots, x_{n+1})$. Alors l'extension $\mathbb{K}(x_{n+1})$ est fini de degré le degré du polynôme minimale de x_{n+1} sur $\mathbb{K}$. Ainsi par hypothèse de récurrence et théorème de la base télescopique on a : $[\mathbb{K}(x_1, \ldots, x_{n+1}) : \mathbb{K}] = [\mathbb{K}(x_1, \ldots, x_{n+1}) : \mathbb{K}(x_{n+1})][\mathbb{K}(x_{n+1}) : \mathbb{K}]$.

Définition 25. *Le corps $\mathbb{K}$ est dit **algébriquement clos** si tout polynôme non constant à coefficients dans $\mathbb{K}$ admet une racine dans $\mathbb{K}$.*

Proposition 41. *Les corps algébriquement clos sont ceux qui n'ont aucune extension finie non triviale.*

Démonstration.
En effet, si $\mathbb{K}$ est un corps algébriquement clos, $\mathbb{L}/\mathbb{K}$ une extension finie et $x \in \mathbb{L}$, alors $\Pi_{K,x}$ est un irréductible de $\mathbb{K}[X]$, donc de degré 1 donc $x \in \mathbb{K}$. Réciproquement, si $\mathbb{K}$ n'est pas algébriquement clos, on peut trouver $P \in \mathbb{K}[X]$ irréductible sur $\mathbb{K}$ de degré $n \geq 2$; si x est une racine de P dans un extension de $\mathbb{K}$, $\mathbb{K}(x)/\mathbb{K}$ est une extension finie de degré n.

On se propose d'étudier quelques résultats sur les nombres algébriques dans différents corps.

Proposition 42. *Soit x un nombre complexe algébrique sur $\mathbb{Q}$. Alors est x un entier algébrique (ie algébrique sur $\mathbb{Z}$) si et seulement si $\Pi_{\mathbb{Q},x}$ appartient à $\mathbb{Z}[X]$.*

Démonstration. Nous aurons besoin du lemme suivant :

Lemme 8.

(i) Lemme de Gauss : Si P et Q sont dans $\mathbb{Z}[X]\backslash\{0\}$, $C(PQ) = C(P)C(Q)$ où $C(P)$ désigne le pgcd des coefficients du polynômes P.

(ii) Soit $P \in \mathbb{Z}[X]\backslash\{0\}$. Si $P = P_1P_2$ avec $P_1, P_2 \in \mathbb{Q}[X]$, il existe Q_1, Q_2 dans $\mathbb{Z}[X]$, associés respectivement à P_1 et P_2 dans $\mathbb{Q}[X]$ tels que $P = C(P)Q_1Q_2$.

Si $i \in \{1, 2\}$, on écrit $P_i = \frac{u_i}{v_i}Q_i$ avec $u_i, v_i \in \mathbb{Z}\backslash\{0\}$ et $Q_i \in \mathbb{Z}[X]$ avec $C(Q) = 1$. Alors : $u_1u_2Q_1Q_2 = v_1v_2P$ ($C(Q_1Q_2) = 1$ car $C(Q_1) = C(Q_2) = 1$) et d'après le lemme de Gauss : $u_1u_2 = \pm C(P)v_1v_2$.
Il suffit de prouver que, si un polynôme unitaire P de $\mathbb{Z}[X]$ admet x comme racine, alors $\Pi_{\mathbb{Q},x}$ appartient à $\mathbb{Z}[X]$. D'après le lemme il existe $\Gamma \in \mathbb{Z}[X]$ associé à $\Pi_{\mathbb{Q},x}$ et divisant P dans $\mathbb{Z}[X]$. Comme P est unitaire, $\pm\Gamma$ l'est aussi. Il en résulte que $\Pi_{Q,x} = \pm\Gamma \in \mathbb{Z}[X]$.

Proposition 43. *Cas des extensions quadratiques : Soient $a \in \mathbb{K}$ non carré, x une racine carrée de a dans une extension. Alors $\mathbb{K}(x)$ est une extension de degré 2 (ou quadratique) de $\mathbb{K}$ que l'on note $\mathbb{K}(\sqrt{a})$. Inversement, si $\mathbb{K}$ n'est pas de caractéristique 2 et si $\mathbb{L}$ est une extension de degré 2 de $\mathbb{K}$, $\exists a \in \mathbb{K}$ tel que $\mathbb{L} = \mathbb{K}(\sqrt{a})$.*

Démonstration. Soit en effet $x \in \mathbb{L}\backslash\mathbb{K}$. Montrons $\mathbb{L} = \mathbb{K}(x)$. On a déjà l'inclusion triviale $\mathbb{K}(x) \subset$ $\mathbb{L}$.z De plus le théorème de la base télescopique assure que $2 = [\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}(x)][\mathbb{K}(x) : \mathbb{K}]$ donc $[\mathbb{K}(x) : \mathbb{K}] = 1$ ou $[\mathbb{K}(x)] : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]$. Le premier cas est exclu, car on a $\mathbb{K}(x) \neq \mathbb{K}$ donc $[\mathbb{K}(x) : \mathbb{K}] = [\mathbb{L} : \mathbb{K}]$ et $[\mathbb{L} : \mathbb{K}(x)] = 1$. L'extension est quadratique donc le degré du polynôme minimal de x est 2. $\exists a, b \in \mathbb{K}$ tel que $\Pi_{\mathbb{K},x} = X^2 + aX + b$. On a donc $x^2 + ax + b = 0$.comme $\mathbb{K}$ n'est pas de caractéristique 2, nous pouvons compléter le carré. Soit $\delta = \frac{b^2-4c}{4} \in \mathbb{K}$, on a alors $\Pi_{\mathbb{K},x} = (x+\frac{b}{2})^2-\delta$ ainsi $x+\frac{b}{2}$ est une racine de δ comme $\frac{b}{2} \in \mathbb{K}$, on a $\mathbb{L} = \mathbb{K}(x) = \mathbb{K}(x+\frac{b}{2}) = \mathbb{K}(\sqrt{\delta})$.

Proposition 44. *Soient $a, b \in \mathbb{K}\backslash\{0\}$ non carré de $\mathbb{K}$ de caractéristique différente de 2, $\mathbb{K}(\sqrt{a}) = \mathbb{K}(\sqrt{b}) \iff \frac{b}{a}$ est un carré dans $\mathbb{K}$.*

Démonstration. Sens direct : on suppose que $\mathbb{K}(\sqrt{a}) = \mathbb{K}(\sqrt{b})$. On a donc que $\sqrt{b} = x + y\sqrt{a}$ avec $x, y \in \mathbb{K}$. Il suffit de regrouper les puissances paires et impaires. On a donc $(b - x^2 - ay^2)^2 = 4x^2y^2a$ or a n'est pas un carré dans $\mathbb{K}$ donc $2xy = 0$ donc en développant le carré on obtient $b = x^2 + ay^2$ or $2 \neq 0$ et b n'est pas un carré dans $\mathbb{K}$ donc $x = 0$ donc $\frac{b}{a} = y^2 \in \mathbb{K}$.
Réciproquement, si $\frac{b}{a} = x^2$ pour un $x \in \mathbb{K}$. On a a $\sqrt{b} = \pm x\sqrt{a}$ et $\mathbb{K}(\sqrt{a}) = \mathbb{K}(\sqrt{b})$.

Définition 26. *L'extension $\mathbb{L}/\mathbb{K}$ est dite **algébrique** si tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.*

Théorème 9. *Transitivité de l'algébricité : Soient $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$ deux extensions de corps. Alors $\mathbb{M}/\mathbb{K}$ est algébrique si et seulement si $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$ sont algébriques.*

Démonstration. Le sens indirect est triviale. Pour le sens direct : supposons $\mathbb{M}/\mathbb{L}$ et $\mathbb{L}/\mathbb{K}$ algébriques. Soient $x \in \mathbb{M}$ et $\mathbb{K}'$ le sous-corps de $\mathbb{L}$ engendré par $\mathbb{K}$ et les coefficients de $\Pi_{\mathbb{L},x}$. L'extension $\mathbb{K}'/\mathbb{K}$ est finie (car chacun des coefficients du polynôme minimal sont algébriques sur $\mathbb{K}$ donc $\mathbb{K}'/\mathbb{K} = \mathbb{K}(a_0, \ldots, a_n)/\mathbb{K}$ est fini d'après la proposition 37) et x est algébrique sur $\mathbb{K}'$ par construction. L'extension $\mathbb{K}'(x)/\mathbb{K}$ est donc également finie ; a fortiori, $\mathbb{K}(x)/\mathbb{K}$ est finie et x est algébrique sur $\mathbb{K}$.

Corollaire 8. *Soient $\mathbb{K}$ corps, Ω un surcorps algébriquement clos de $\mathbb{K}$, l'ensemble $\mathbb{L}$ des éléments de Ω algébriques sur $\mathbb{K}$. Alors $\mathbb{L}$ est un sous-corps algébriquement clos de Ω.*

Démonstration. On sait déjà que $\mathbb{L}$ est un sous-corps de Ω. Soit $P \in \mathbb{L}[X]$ unitaire non constant :

$$P = X^n + \sum_{i=0}^{n-1} a_i X^i.$$

Soit x une racine de P dans Ω. x est algébrique sur $\mathbb{K}(a_0, \ldots, a_{n-1})$, qui est une extension finie de $\mathbb{K}$. Par transitivité, x est algébrique sur $\mathbb{K}$, d'où $x \in \mathbb{L}$. On admet le théorème suivant :

Théorème 10. *Théorème de l'élément primitif : Supposons $\mathbb{K}$ de caractéristique nulle et $\mathbb{L}/\mathbb{K}$ finie. Alors $\mathbb{L}/\mathbb{K}$ est monogène.*

Ce dernier assure une simplification pour un grand nombres de preuves de la théorie de Galois.

Définition 27. *Soit $\mathbb{L}/\mathbb{K}$ une extension. Un élément x de $\mathbb{L}$ est séparable sur $\mathbb{K}$ s'il est algébrique sur $\mathbb{K}$ et si $\Pi_{\mathbb{K},x}$ est séparable, c'est-à-dire premier avec sa dérivée.*
L'extension $\mathbb{L}/\mathbb{K}$ est séparable si tout élément x de $\mathbb{L}$ est séparable sur $\mathbb{K}$, ce qui impose que $\mathbb{L}/\mathbb{K}$ est algébrique.
Si $\mathbb{K}$ est de caractéristique nulle, toute extension algébrique $\mathbb{L}/\mathbb{K}$ est séparable. Il en est plus généralement de même si $\mathbb{K}$ est parfait.

Théorème 11. *Soient $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$ deux extensions finies. Si $\mathbb{M}/\mathbb{K}$ est séparable, alors $\mathbb{L}/\mathbb{K}$ et $\mathbb{M}/\mathbb{L}$ le sont.*

5.1.2 Surcorps

La majorité des propositions concernant l'étude de l'irréductibilité d'un polynôme $P \in \mathbb{K}[X]$ requiert l'existence d'un surcorps de $\mathbb{K}$ scindant P. Il est donc naturel de justifier l'existence de

ce dernier.

Proposition 45. *Soit P un polynôme irréductible de $\mathbb{K}[X]$. Il existe une extension $\mathbb{K}'$ de $\mathbb{K}$ telle que :*

(i) P a une racine $x \in \mathbb{K}'$

(ii) $\mathbb{K}' = \mathbb{K}(x)$

Démonstration. Il suffit de considérer $\mathbb{K}' = \mathbb{K}[X]/(P)$.
Un tel corps vérifiant (i) et (ii) est appelé **corps de rupture de P sur $\mathbb{K}$**.

Proposition 46. *Soit $P \in \mathbb{K}[X]$ non constant. Il existe une extension $\mathbb{L}$ de $\mathbb{K}$ telle que :*

(i) P est scindé sur $\mathbb{L}$,

(ii) si $\mathcal{R}$ est l'ensemble des racines de P dans $\mathbb{L}$, alors $\mathbb{L} = \mathbb{K}(\mathcal{R})$.

Démonstration. On raisonne par récurrence sur le degré d de P.

Un tel corps vérifiant (i) et (ii) est appelé **corps de décomposition de P sur $\mathbb{K}$**.

Proposition 47. *Soit P un polynôme non constant dans $\mathbb{K}[X]$ et $\mathbb{L}$ un corps de décomposition de P sur $\mathbb{K}$.*

1. *Si P est de degré n, alors $[\mathbb{L} : \mathbb{K}]$ divise $n!$.*
2. *Supposons que P soit réductible sur $\mathbb{K}$, c'est-à-dire $P = UV$ avec U et V dans $\mathbb{K}[X]$ de degrés respectifs d et $n-d$, où $1 \leq d \leq n-1$. Alors $[\mathbb{L} : \mathbb{K}]$ divise $d!(n-d)!$ et est donc majoré par $(n-1)!$.*

Démonstration.
On raisonne par récurrence sur n. $n = 1$ est trivial.
Supposons $n \geq 2$ et le résultat vrai pour P de degré au plus $n-1$. Soient P dans $\mathbb{K}[X]$ de degré n, $\mathbb{L}$ un corps de décomposition de P sur $\mathbb{K}$. On distingue deux cas.
Premier cas : P est réductible sur $\mathbb{K}$
Si P s'écrit $P = UV$ avec U et V dans $\mathbb{K}[X]$ non constants. Notons d le degré de U, $\mathcal{R}$ (resp. $\mathcal{R}'$) l'ensemble des racines de U (resp. V) dans $\mathbb{L}$. On a

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{K}(\mathcal{R}) : \mathbb{K}] \times [\mathbb{L} : \mathbb{K}(\mathcal{R})].$$

Mais $\mathbb{K}(\mathcal{R})$ est un corps de décomposition de U sur $\mathbb{K}$, tandis que $\mathbb{L} = \mathbb{K}(\mathcal{R} \cup \mathcal{R}')$ est un corps de décomposition de V sur $\mathbb{K}(\mathcal{R})$. L'hypothèse de récurrence montre que $[\mathbb{K}(\mathcal{R}) : \mathbb{K}]$ divise $d!$ et que $[\mathbb{L} : \mathbb{K}(\mathcal{R})]$ divise $(n-d)!$. Par conséquent, $[\mathbb{L} : \mathbb{K}]$ divise $d!(n-d)!$, lequel divise $n!$ puisque $\binom{n}{d}$ est entier.
Deuxième cas : P est irréductible sur $\mathbb{K}$
Notons $x_1, \ldots, x_n$ les racines de P dans $\mathbb{L}$ comptées avec multiplicité. On considère le polynôme

$$Q = \prod_{i=1}^{n-1}(X - x_i) = \frac{P}{X - x_n}.$$

Alors Q appartient à $\mathbb{K}(x_n)[X]$ et est de degré $n-1$; de plus, $\mathbb{L}$ est un corps de décomposition de Q sur $\mathbb{K}(x_n)$. L'hypothèse de récurrence entraîne que $[\mathbb{L} : \mathbb{K}(x_n)]$ divise $(n-1)!$. Comme $[\mathbb{K}(x_n) : \mathbb{K}] = n$ ($\Pi_{\mathbb{K},x_n} = P$ par irréductibilité de P), on conclut par multiplicativité des degrés.
Preuve de ii). L'argument justifiant la première assertion a été donné dans la preuve de i). La seconde provient du fait que la suite $\binom{n}{d}$ pour $1 \leq d \leq n/2$ est croissante et de la relation de symétrie

$$\forall d \in \{0, \dots, n\}, \quad \binom{n}{d} = \binom{n}{n-d}.$$

Définition 28. *Soit $\mathbb{R}$ un anneau commutatif, on appelle **corps résiduel** de R le quotient de R par un de ces ideaux maximaux.*

5.1.3 Morphisme et conjugaison

Nous pouvons remarquer que si nous considérer $\mathbb{L}/\mathbb{K}$ une extension, $P \in \mathbb{K}[X]$ et $x \in \mathbb{L}$ une racine de P alors pour tout endomorphisme σ de $\mathbb{L}$, $\sigma(x)$ est une racine de P. On peut donc s'intéresser à l'action d'un tel morphisme sur les racines des polynômes.

Définition 29. *Si $\mathbb{L}$ et $\mathbb{M}$ sont deux sous-corps de Ω, on note $Hom(\mathbb{L}, \mathbb{M})$ l'ensemble des morphismes de corps de $\mathbb{L}$ dans $\mathbb{M}$. Si A, A' sont deux $\mathbb{K}$-algèbres, on note $Hom_{\mathbb{K}}(A, A')$ l'ensemble des morphismes de $\mathbb{K}$-algèbres de A dans A'. Si $\mathbb{L}$ et $\mathbb{M}$ sont deux extensions de $\mathbb{K}$, $Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{M})$ est donc l'ensemble des éléments de $Hom(\mathbb{L}, \mathbb{M})$ qui induisent l'identité sur $\mathbb{K}$.*

Proposition 48. *Si $\mathbb{K}$ est l'un des sous-corps premiers $\mathbb{Q}$ ou $\mathbb{F}_p$ avec p premier et $\mathbb{L}$ une extension de $\mathbb{K}$, il n'y a qu'un élément de $Hom(\mathbb{K}, \mathbb{L})$, à savoir l'inclusion de $\mathbb{K}$ dans $\mathbb{L}$, ceci parce qu'un morphisme d'anneau envoie 1 sur 1. Par conséquent, si $\mathbb{K}$ est l'un de ces corps et $\mathbb{L}, \mathbb{M}$ deux extensions de $\mathbb{K}$, on a $Hom(\mathbb{L}, \mathbb{M}) = Hom_{\mathbb{K}}(\mathbb{L}, \mathbb{M})$.*

Définition 30. *Si $P = \sum_{i=0}^{n} a_i X^i$ est dans $\mathbb{K}[X]$, et si σ est un morphisme de corps de $\mathbb{K}$ dans $\mathbb{K}'$, on note $\sigma.P$ le polynôme :*

$$\sigma.P = \sum_{i=0}^{n} \sigma(a_i) X^i$$

.

L'application $P \mapsto \sigma.P$ est l'unique prolongement de σ en un morphisme d'anneaux de $\mathbb{K}[X]$ dans $\mathbb{K}'[Y]$ envoyant X sur Y . Cette propriété entraîne que P est irréductible sur $\mathbb{K}$ si et seulement si $\sigma.P$ l'est sur $\sigma(K)$.

Lemme 9. *Soient A et A' deux $\mathbb{K}$-algèbres commutatives, σ une application de A dans A'. Les deux notions suivantes sont équivalentes.*

i) L'application σ est un morphisme de $\mathbb{K}$-algèbres.

ii) Pour tout élément n de $\mathbb{N}^*$, tout P de $\mathbb{K}[X_1, \dots, X_n]$ et tout $(x_1, \dots, x_n)$ de A^n :

$$\sigma(P(x_1, \dots, x_n)) = P(\sigma(x_1), \dots, \sigma(x_n)).$$

Si ces conditions sont réalisées, on a :
$P(x_1, ..., x_n) = 0 \implies P(\sigma(x_1), ..., \sigma(x_n)) = 0.$

Définition 31. *Deux éléments x et y d'une extension de $\mathbb{K}$ sont dits conjugués sur $\mathbb{K}$, ou $\mathbb{K}$-conjugués, s'ils sont algébriques sur $\mathbb{K}$ et vérifient $\Pi_{\mathbb{K},x} = \Pi_{\mathbb{K},y}$.*
L'ensemble des $\mathbb{K}$-conjugués dans Ω d'un élément x de Ω est donc fini de cardinal majoré par $\deg(\Pi_{\mathbb{K},x}) = [\mathbb{K}(x) : \mathbb{K}]$, avec égalité si et seulement si x est séparable sur $\mathbb{K}$.

Proposition 49. *Soient x et y deux éléments d'une extension $\mathbb{L}$ de $\mathbb{K}$, avec x algébrique sur $\mathbb{K}$. Les deux assertions suivantes sont équivalentes.*

i) Il existe $\sigma \in Hom_{\mathbb{K}}(\mathbb{K}(x), \mathbb{L})$ tel que $\sigma(x) = y$.

ii) Les éléments x et y sont $\mathbb{K}$-conjugués.

Dans ce cas, σ est unique et induit un isomorphisme de $\mathbb{K}(x)$ sur $\mathbb{K}(y)$.

Démonstration. On suppose qu'il existe un morphisme de $\mathbb{K}$-algèbres σ de $\mathbb{K}(x) = \mathbb{K}[x]$ sur $\mathbb{K}(y)$ envoyant x sur y, grâce au lemme précédent, on a :

$$\forall P \in \mathbb{K}[X], \sigma(P(x)) = P(y),$$

ce qui en établit l'unicité. On en déduit que $\Pi_{\mathbb{K},x}$ annule y, donc que y est algébrique sur $\mathbb{K}$ et que $\Pi_{\mathbb{K},y} = \Pi_{\mathbb{K},x}$ par irréductibilité du polynôme minimal. Ainsi x et y sont $\mathbb{K}$-conjugués.
Supposons désormais que $\Pi_{\mathbb{K},x} = \Pi_{K,y}$. Alors, pour P et Q dans $\mathbb{K}[X]$, on a :

$$P(x) = Q(x) \Rightarrow \Pi_{\mathbb{K},x} \mid (P - Q) \Rightarrow \Pi_{\mathbb{K},y} \mid (P - Q) \Rightarrow P(y) = Q(y).$$

Posons donc

$$\forall P \in \mathbb{K}[X], \sigma(P(x)) = P(y),$$

on définit bien une application de $\mathbb{K}[x] = \mathbb{K}(x)$ dans $\mathbb{K}[y] = \mathbb{K}(y)$. Il est immédiat de vérifier que cette application appartient à $\mathrm{Hom}_{\mathbb{K}}(\mathbb{K}(x), \mathbb{K}(y))$ et est bijective.

Théorème 12. *Soient $\mathbb{K}$, $\mathbb{K}'$ deux corps, $\mathbb{L}/\mathbb{K}$ et $\mathbb{L}'/\mathbb{K}'$ deux extensions, σ un isomorphisme de $\mathbb{K}$ sur $\mathbb{K}'$, x un élément de $\mathbb{L}$ algébrique sur $\mathbb{K}$ et x' un élément de $\mathbb{L}'$. Les deux assertions suivantes sont équivalentes.*

i) Il existe $\sigma' \in Hom(\mathbb{K}(x), \mathbb{L}')$ prolongeant σ et envoyant x sur x'.

ii) L'élément x' est algébrique sur $\mathbb{K}'$, et $\Pi_{\mathbb{K}',x'} = \sigma(\Pi_{\mathbb{K},x})$.

Si ces conditions sont réalisées, le prolongement donné par i) est unique, et induit un isomorphisme du corps $\mathbb{K}(x)$ sur le corps $\mathbb{K}'(x')$.

Démonstration. Si i) est vérifiée, alors

$$\forall P \in \mathbb{K}[X], \sigma'(P(x)) = \sigma.P(x').$$

Ceci prouve que x' est algébrique sur $\mathbb{K}'$ et que $\Pi_{\mathbb{K}',x'}$ divise $\sigma.\Pi_{\mathbb{K},x}$, d'où l'égalité de ces deux polynômes car tous deux irréductibles sur $\mathbb{K}$ resp $\mathbb{K}'$. Réciproquement, si ii) est réalisée, l'application :

$$\Phi : \mathbb{K}[X] \to \mathbb{L}' \quad P \mapsto \sigma.P(x')$$

définit un morphisme d'anneaux de noyau engendré par $\Pi_{\mathbb{K},x}$. Ceci permet de définir, par passage au quotient, un morphisme d'anneaux σ' de $\mathbb{K}[x]$ dans $\mathbb{L}'$ en posant :

$$\forall P \in \mathbb{K}[X], \sigma'(P(x)) = \sigma.P(x').$$

Ce morphisme prolonge σ et induit clairement une bijection de $\mathbb{K}(x)$ sur $\mathbb{K}'(x')$.
Si $\mathbb{L}' = \Omega$, on dispose d'une racine x' de $\sigma.\Pi_{\mathbb{K},x}$ dans Ω et donc d'au moins un prolongement de σ en un élément de $\mathrm{Hom}(\mathbb{K}(x), \Omega)$. En notant qu'une extension finie de $\mathbb{K}$ est engendrée par un nombre fini d'éléments algébriques sur $\mathbb{K}$, il suffit donc de faire une récurrence sur le nombre d'éléments constituant l'extension pour conclure.

5.1.4 Théorie de Galois

Dans ce sous-chapitre nous nous intéresserons à la théorie de Galois proprement dite. Le contexte est le suivant : on considère un corps $\mathbb{K}$ et une clôture algébrique Ω de $\mathbb{K}$. On suppose que toutes les extensions algébriques de $\mathbb{K}$ considérées ici seront supposées plongées dans Ω.

Définition 32. *Soit $\mathbb{L}/\mathbb{K}$ est une extension de corps, on remarque que l'ensemble des automorphismes de la $\mathbb{K}$-algèbre $\mathbb{L}$ est un sous-groupe du groupe des bijections de $\mathbb{L}$ sur lui-même. On l'appelle* ***groupe de Galois de l'extension*** *$\mathbb{L}/\mathbb{K}$ et on le note $Gal(\mathbb{L}/\mathbb{K})$. Les éléments de $Gal(\mathbb{L}/\mathbb{K})$ sont donc les bijections de $\mathbb{L}$ sur lui-même qui respectent les relations algébriques à coefficients dans $\mathbb{K}$.*

5.2 Théorie de Galois et corps p-adique

5.2.1 Clôture algébrique d'un corps valué complet et prolongement

Définition 33. *Deux normes sur un corps $\mathbb{K}$ sont dites équivalentes si elle définissent la même topologie.*

Proposition 50. *Deux normes $||.||_1$ et $||.||_2$ sont équivalentes si et seulement si il existe $s \in \mathbb{R}_+^*$ tel que $||x||_1 = ||x||_2^s \ \forall x \in \mathbb{K}^*$.*

Démonstration. Si $\|\cdot\|$ est une norme sur le corps $\mathbb{K}$, alors $|x| < 1$ si et seulement si la suite de terme général x^n tend vers 0 quand n tend vers $+\infty$. On en déduit que si $\|\cdot\|_1$ et $\|\cdot\|_2$ sont équivalentes, alors

$$\{x \in \mathbb{K} \mid \|x\|_1 < 1\} = \{x \in \mathbb{K} \mid \|x\|_2 < 1\}.$$

Si ce dernier ensemble est réduit à $\{0\}$, on a $\|x\|_1 = \|x\|_2 = 1$ quel que soit $x \in \mathbb{K}^*$. Sinon, soit $x \in \mathbb{K}^*$ vérifiant $\|x\|_1 < 1$. Si $y \in \mathbb{K}^*$, $a \in \mathbb{Z}$ et $b \in \mathbb{N}$, alors

$$\|y^b x^{-a}\|_1 < 1 \iff \|y^b x^{-a}\|_2 < 1.$$

On en déduit que

$$\{r \in \mathbb{Q} \mid r < \frac{\log \|y\|_1}{\log \|x\|_1}\} = \{r \in \mathbb{Q} \mid r < \frac{\log \|y\|_2}{\log \|x\|_2}\}$$

et $\frac{\log \|y\|_1}{\log \|x\|_1}$ et $\frac{\log \|y\|_2}{\log \|x\|_2}$ définissent la même coupure de Dedekind et sont donc égaux, ce qui montre que la fonction $y \mapsto \frac{\log \|y\|_1}{\log \|y\|_2}$ est constante sur $\mathbb{K}^*$ et on en déduit aisément le résultat.

Proposition 51. *Soit $\mathbb{K}$ un corps normé complet et V un espace vectoriel de dimension finie sur $\mathbb{K}$, alors toutes les normes sur V (compatibles avec la norme sur $\mathbb{K}$, i.e. vérifiant $||\lambda x|| = |\lambda| \times ||x||$ si $\lambda \in \mathbb{K}$ et $x \in V$) sont équivalentes et V est complet pour n'importe laquelle d'entre elles.*

Démonstration. Il suffit de prouver qu'elles sont toutes équivalentes à la norme du sup, on raisonne alors par récurrence sur la dimension de V. Si cette dimension est 1, le résultat est clair.
Sinon, soit $e_1, \dots, e_n$ une base de V; on a

$$\|x_1 e_1 + \cdots + x_n e_n\| \leq (\|e_1\| + \cdots + \|e_n\|) \sup(|x_1|, \dots, |x_n|),$$

d'où l'une des deux inégalités à vérifier. Pour démontrer l'autre, raisonnons par l'absurde. Supposons qu'il existe une suite $x_1^{(k)} e_1 + \cdots + x_n^{(k)} e_n$ qui tende vers 0 pour la norme $\|\cdot\|$ mais pas pour la norme du sup. Il existe alors $C > 0$, $i \in \{1, \dots, n\}$ et une sous-suite infinie telle que l'on ait $|x_i^{(k)}| > C$ et donc la suite de terme général

$$v_k = \frac{x_1^{(k)}}{x_i^{(k)}} e_1 + \cdots + \frac{x_n^{(k)}}{x_i^{(k)}} e_n$$

tend encore vers 0 pour $\|\cdot\|$. Ainsi e_i est dans l'adhérence de $W = \mathrm{Vect}(e_1, \dots, e_{i-1}, e_{i+1}, \dots, e_n)$ qui est complet d'après l'hypothèse de récurrence, ce qui implique $e_i \in W$ et est absurde puisque les e_i forment une base de V.

Définition 34. *Soit $\mathbb{L}/\mathbb{K}$ une extension finie d'un corps $\mathbb{K}$, et $x \in \mathbb{L}$. On définit la norme de x de $\mathbb{L}$ sur $\mathbb{K}$, $N_{\mathbb{L}/\mathbb{K}}(x)$, comme :*

- *le déterminant de l'endomorphisme $y \mapsto xy$. De la même manière, on définit la trace de x de $\mathbb{L}$ sur $\mathbb{K}$, $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x)$, comme la trace de ce même endomorphisme.*
- *Si $P = X^n + \cdots + a_0$ est le polynôme minimal unitaire de x sur $\mathbb{K}$ et $r = [\mathbb{L} : \mathbb{K}(\alpha)]$, alors $N_{\mathbb{L}/\mathbb{K}}(x) = (-1)^{nr} a_0^r$.*
- *Si l'extension $\mathbb{L}/\mathbb{K}$ est normal, alors $N_{\mathbb{L}/\mathbb{K}}(x) = \Pi_{\sigma \in Aut(\mathbb{L}/\mathbb{K})}\sigma(x)$*

Ces 3 définitions sont équivalentes et peuvent être utilisés dans différents contextes.

Démonstration. Démontrons l'équivalence de ces 3 propositions.
On peut remarquer que la première et dernière définitions imposent le caractère multiplicatif de la norme. De plus, on peut remarquer que si $\alpha \in \mathbb{K}$, on a $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha^{[\mathbb{L}:\mathbb{K}]}$ par exemple d'après la première définition.
On peut remarquer que les deux premières définitions sont équivalentes lorsque le surcorps est $\mathbb{K}(\alpha)$ avec $\alpha \in \mathbb{L}$. En effet, si on note $n = [\mathbb{K}(\alpha) : \mathbb{K}]$ une base de $\mathbb{K}(\alpha)$ est $\{1, \alpha, \ldots, \alpha^{n-1}\}$ et la matrice associée à la multiplication par α dans cette base est une matrice compagnon de polynôme caractéristique le polynôme minimal de α sur $\mathbb{K}$. On en déduit le résultat par les relations coefficients racines. Prouvons que les deux premières définitions sont encore équivalentes; pour cela nous avons besoin de prouver la transitivité des normes :

Lemme 10. *Transitivité des normes : Soient $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ 3 extensions finies. Alors $\forall \alpha \in \mathbb{M}$, $N_{\mathbb{M}/\mathbb{K}}(\alpha) = N_{\mathbb{L}/\mathbb{K}}(N_{\mathbb{M}/\mathbb{L}}(\alpha))$.*

A priori cette norme semble sortir de nul part pourtant elle sera très utile dans la suite. En effet, soit $\mathbb{K}$ une extension normale de $\mathbb{Q}_p$ et soit σ un automorphisme de $\mathbb{K}$ et $|.|$ une valeur absolue sur $\mathbb{K}$. L'application $|\sigma(.)|$ est aussi une valeur absolue sur $\mathbb{K}$ qui converse la valeur absolue p-adique sur $\mathbb{Q}_p$ car σ y induit l'identité. Or nous avons montré qu'il n'y a qu'une seule valeur absolue pareille. Ainsi $|\sigma(x)| = |x| \forall x \in \mathbb{K}$. Si on note n le degré de l'extension (qui est normale) on a donc $|x|^n = |\Pi_\sigma \sigma(x)|$ donc par définition de la norme on a : $|x| = \sqrt[n]{|N_{\mathbb{K}/\mathbb{Q}_p}(x)|}$

Lemme 11. *Soient $\mathbb{L}$ et $\mathbb{K}$ deux extensions finis de $\mathbb{Q}_p$ avec $\mathbb{Q}_p \subset \mathbb{K}\mathbb{L}$. Soit $x \in \mathbb{K}$. Soient $m = [\mathbb{L} : \mathbb{Q}_p]$ et $n = [\mathbb{K} : \mathbb{Q}_p]$. On a : $\sqrt[m]{|N_{\mathbb{L}/\mathbb{Q}_p}(x)|_p} = \sqrt[n]{|N_{\mathbb{K}/\mathbb{Q}_p}(x)|_p}$*

Proposition 52. *S'il existe une valeur absolue /./ sur un corps $\mathbb{K}$ prolongeant la valeur absolue p-adique, alors on a nécessairement $|x| = \sqrt[n]{|N_{\mathbb{K}/\mathbb{Q}_p}(x)|_p}$ où $n = [\mathbb{K} : \mathbb{Q}_p]$.*

Ce résultat est plus général comme le montre le théorème suivant :

Théorème 13. *Soit $\mathbb{K}$ un corps complet pour une valuation v, et soit $\mathbb{L}$ une extension finie de $\mathbb{K}$. Alors, il existe une unique manière de prolonger v en une valuation de $\mathbb{L}$. De plus, si $x \in \mathbb{L}$, alors*

$$v(x) = \frac{1}{[\mathbb{L} : \mathbb{K}]} v(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)).$$

Proposition 53. *Soit $f \in \mathbb{K}[X]$ un polynôme unitaire irréductible vérifiant $f(0) \in \mathcal{O}_\mathbb{K}$. Alors tous les coefficients de f appartiennent à $\mathcal{O}_\mathbb{K}$.*

Démonstration.
On peut voir $\mathbb{L}$ comme un $\mathbb{K}$-espace vectoriel de dimension finie $[\mathbb{L} : \mathbb{K}]$. Si v_1, v_2 sont deux valuations sur $\mathbb{L}$ prolongeant v, alors v_1 et v_2 définissent la même topologie sur $\mathbb{L}$ d'après la proposition 45. La proposition 44 montre alors qu'il existe $s \in \mathbb{R}_+^*$ tel que l'on ait

$$v_2(x) = s \cdot v_1(x) \quad \text{quel que soit } x \in \mathbb{L},$$

et comme $v_1(x) = v_2(x)$ si $x \in \mathbb{K}$, on en déduit que $s = 1$ et donc l'unicité d'une extension de v à $\mathbb{L}$.
Il reste à montrer que la formule ci-dessus définit bien une valuation sur $\mathbb{L}$. On remarque qu'il reste à vérifier le dernier axiome d'une valuation ie que si $v(\alpha + \beta) \geq \inf(v(\alpha), v(\beta))$ et quitte à supposer $\alpha \neq \beta$ on peut intervertir α et β on peut supposer $v(\alpha) \leq v(\beta)$ et sans perte de généralités à soustraire par $v(\alpha)$ on peut juste prouver que si $x \in \mathbb{L}$ vérifie $v(\mathrm{N}_{L/\mathbb{K}}(x)) > 0$, alors $v(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(1 + x)) > 0$.
Soit $f(X) = X^d + \cdots + a_0$, le polynôme minimal de x sur $\mathbb{K}$. Ceci implique que d divise $[L : \mathbb{K}]$ et $\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x) = ((-1)^d a_0)^{[\mathbb{L}:\mathbb{K}]/d}$ donc $v(\mathrm{N}_{\mathbb{L}/\mathbb{K}}(x)) > 1$ implique $a_0 \in \mathcal{O}_\mathbb{K}$ et l'irréductibilité de f implique que f est à coefficients dans $\mathcal{O}_\mathbb{K}$ d'après la proposition 46. D'autre part, le polynôme minimal de $1 + x$ est $f(X - 1)$ et donc

$$\mathrm{N}_{\mathbb{L}/\mathbb{K}}(1 + x) = ((-1)^d f(-1))^{[\mathbb{L}:\mathbb{K}]/d} \in \mathcal{O}_\mathbb{K},$$

ce qui permet de conclure.

Proposition 54. *Le corps $\mathbb{Q}_p$ n'est pas algébriquement clos.*

Démonstration. Il suffit de considérer par exemple les racines du polynôme $P(X) = X^2 - p^7 \in \mathbb{Q}_p[X]$.

Pour pouvoir faire convenablement de l'analyse, il semble naturel de considère une clôture algébrique de $\mathbb{Q}_p$, que l'on note $\overline{\mathbb{Q}_p}$ et qui n'est pas complète. Nous avons donc besoin de la compléter pour former un plus grand corps cet fois-ci complet, algébriquement clôs que l'on note $\mathbb{C}_p$ et muni d'une norme p-adique (qu'on notera encore $|.|_p$), qui prolonge celle définit sur $\mathbb{Q}_p$:
$\forall x \in \mathbb{C}_p, \quad |x|_p = \lim_{n \to +\infty} |x_n|_p$, où $(x_n)_{n \geq 0}$ est une suite de Cauchy d'éléments de $\mathbb{Q}_p$.

Proposition 55. *Le corps $\mathbb{C}_p$ vérifie les propriétés suivantes :*

(i) $\mathbb{C}_p$ est algébriquement clos.

(ii) Le corps $\mathbb{C}_p$ n'est pas localement compact.

(iii) Le corps $\mathbb{C}_p$ est séparable.

Démonstration. Nous allons prouver le point (i) grâce au lemme de Krasmer :

Lemme 12. *Soit $\mathbb{K}$ un corps valué complet. Soit $\alpha, \beta \in \mathbb{K}^{alg}$, avec α séparable sur $\mathbb{K}(\beta)$ (i.e le polynôme minimal de α dans $\mathbb{K}^{alg}$ est à racines simples). Supposons que pour tout conjugué $\alpha_i \neq \alpha$ de α, on a $|\beta - \alpha| < |\alpha_i - \alpha|$. Alors $\mathbb{K}(\alpha) \subset \mathbb{K}(\beta)$.*

Supposons par l'absurde que α n'appartient pas à $L = \mathbb{K}(\beta)$. On considère donc $L(\alpha)$. Comme $\alpha \notin L$, on a donc $m = [L(\alpha) : L] > 1$. Or on sait qu'il y a m homomorphisme $\Sigma L(\alpha) \to \bar{\mathbb{K}}$ qui est l'identité si co-restreint à L et envoie α sur ses conjugués. Il existe σ_0 tel que $\sigma_0(\alpha) \neq \alpha$. Or par l'unicité de l'extension d'une valeur absolue, on a $|\sigma(x)| = |x| \ \forall \sigma, \forall x \in \bar{\mathbb{K}}$. On a donc $|\sigma_0(\beta) - \sigma_0(\alpha)| = |\beta - \alpha|$. Or $\beta \in L$ donc $\sigma_0(\beta) = \beta$. On a donc $|\beta - \sigma_0(\alpha)| = |\beta - \alpha|$. Par l'inégalité ultramétrique on a donc que $|\alpha - \sigma_0(\alpha)| \leq |\beta - \alpha|$. Ce qui est absurde par nos hypothèses de départ.

6 Autre démonstration du théorème de Skolem-Mahler

On rappelle le théorème de Skolem-Mahler :

Théorème 14. *Soit $(u_n)_{(n\in\mathbb{N})}$ une suite récurrente linéaire entière. Alors en notant $S = \{n \in \mathbb{N} | u_n = 0\}$ alors S est de la forme $\{ensemble finie\} \cup \{réunion\ finie\ de\ suite\ arithmétique\}$.*

Démonstration. Soit $(u_n)_{(n\in\mathbb{N})}$ une suite récurrente linéaire entière de polynôme caractéristique $P = X^n - c_{n-1}X^{n-1} - \ldots - c_0$
ie $u_{n+d+1} = c_{n-1}u_{n+d} + \ldots + c_0 u_n$.
On fixe p premier tel que $p \nmid c_0$. On considère l'ensemble $\mathcal{B}_p = \{(b_n), \exists (d_i) \in \mathbb{Z}^{\mathbb{N}}, b_n = \sum_{i=0}^{n} \binom{n}{i} p^i d_i$.

Montrons qu'il existe $r > 0$, tel que $\forall j \in [\![0, r-1]\!], b_n := u_{nr+j} \in \mathcal{B}_p$. Et que si $(b_n) \in \mathcal{B}_p$ non nulle alors l'ensemble des indices annulant (b_n) est fini.

On sait qu' en notant $U_n = \begin{pmatrix} u_n \\ \vdots \\ u_{n+d-1} \end{pmatrix}$ alors en notant $C = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ c_0 & c_1 & c_2 & c_3 & \cdots & c_{n-1} \end{pmatrix}$ on a $U_{n+1} = CU_n$ donc par récurrence $U_n = C^n U_0$. Et en notant E_i le vecteur colonne avec que des zéros sauf à la ligne i, on a $u_n = {E_1}^T U_n = E_1 C^n U_0$. Dans la réduction des coefficients modulo p, on a $\det(\bar{C}) = \pm\bar{c_0} \neq 0$ par hypothèse. Ainsi $\overline{C} \in GL_d(\mathbb{F}_p)$ qui est un groupe finie. On considère donc r l'ordre de $\overline{C}$, on a donc $C^r = I_d + pD$ avec D une certaine matrice. On a donc $u_{nr+j} = E_1^T C^{nr+j} U_0 = E_1^T (Id + pD)^n C^j U_0 = \sum_{i=0}^{n} \binom{n}{i} p^i E_1^T D^i C^j U_0$. On pose donc $d_i := E_1^T D^i C^j U_0 \in \mathbb{Z}$.
On pose $\forall n \in \mathbb{N}$ le polynôme définie par : $P_n(X) = \sum_{i=0}^{n} \frac{X(X-1)\ldots(X-i+1)}{i!} p^i d_i$, par hypothèse on a $P_n(n) = b_n \ \ \forall n$. On remarque aussi que $\forall n \geq m \ P_n(m) = P_m(m) = b_m$ et que si $x \in Z$, $P_n(x)$ est une $\mathbb{Z}$-combinaison des $\frac{p^i}{i!}$.

Définition 35. *On définit désormais une valuation p-adique filtrée sur les polynômes en définissant $v_p^{(k)}(P) = min_{i\geq k} v_p(a_i)$ si $P = \sum a_i X^i \in \mathbb{Q}[X]$.*

On suppose donc qu'il y a une infinité d'indices annulant la suite (b_n). On considère donc $m_1 < m_2 < \ldots < m_i$ tel que $b_{m_j} = 0$. Soit $n > m_i$, ainsi $P_n(m_j) = 0$ d'après la remarque précédente. Ainsi $\exists Q_n$ tel que $P_n = (X - m_1)\ldots(X - m_i)Q_n$.

Lemme 13. *Si $P = (X - m)Q$, alors $v_p^{(j)}(Q) \geq v_p^{(j+1)}(P)$*

La preuve est la suivante : on a $Q = \frac{P-P(m)}{X-m}$ donc c'est une combinaison des $\frac{X^k-m^k}{X-m} = X^{k-1} + mX^{k-2} + \ldots + m^{k-1}$ donc en notant t_j le coefficient de X^j dans Q est $t_j = s_{j+1} + ms_{j+2} + \ldots + m^{n-j+1}s_n$ où les s_i sont les coefficients de P. Et on a la preuve car $v_p(x + y) \geq min(v_p(x), v_p(y))$.

Par récurrence d'après le lemme on a , $v_p(Q_n) \geq v_p^{(i)}(P_n)$. Or P_n est combinaison linéaire des $\frac{p^j}{j!}$ avec $v_p(\frac{p^j}{j!}) = j - v_p(j!) \geq j - \frac{j}{p-1} = j\frac{p-2}{p-1}$. Ainsi $v_p(Q_n) \geq i\frac{p-2}{p-1}$. Puis $\forall k \leq n, v_p(b_k) = v_p(P_n(k)) \geq v_p(Q_n(k)) \geq v_p(Q_n) \geq i\frac{p-2}{p-1}$ qui tend vers 0 lorsque$i \to +\infty$. Ainsi $\forall k \leq n,\ b_k = 0$, or n est arbitrairement grand donc $b = 0$ absurde. Et ceci prouve le théorème.

Bibliographie

[1] Pierre Colmez. Cours de master2.

[2] Fernando Q. Gouvêa. *p-adic Numbers.* Springer-Verlag, 1997.

[3] Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito. *Fermat's Dream.* American Mathematical Society, 1996. Translated by Masato Kuwata.