UNIVERSITE KASDI MERBAH OUARGLA

Faculté des mathématiques et sciences de la matière

N° d'ordre :
N° de série :

DEPARTEMENT DE MATHEMATIQUES

MASTER

Spécialité : Mathématiques

Option : Algèber et Géométrie

Par :DJEGHOUBBI Imane

Thème

Obstruction au Principe de Hasse

Soutenu publiquement le : 25/05/2017

Devant le jury composé de :

Mr.Mohamed BOUSAID	M.A université de KASDI Merbah - Ouargla	Président
Mr.Med Amine BAHAYOU	M.A. université de KASDI Merbah - Ouargla	Examinateur
Mr.Yassine GUERBOUSSA	M.A. université de KASDI Merbah - Ouargla	Examinateur
Mr.Med Tayeb BENMOUSSA	M.A. université de KASDI Merbah - Ouargla	Examinateur
Mr.Med Laid YOUMBAI	M.A. université de KASDI Merbah - Ouargla	Rapporteur

Dédicaces

Merci ALLAH (mon dieu) de m'avoir donné la capacité d'arriver a ce point, la force d'y écrire,la patience d'aller jusqu'au bout de rêve et le bonheur de lever mes mains vers le ciel et de dire "Ya Kayoum".

c'est avec profonde gratitude et sincères mots, que nous dédions ce modeste travail de fin d'étude a nos chers parents "Djamila et Belkacem", qui ont sacrifie leurs vie pour notre réussite et nous ont éclairé le chemin par leurs conseils judicieux.

Nous dédions aussi ce travail a mes frères "Adel, Malak, Assia, Abd alhamid et Faiza" et ses enfants "Ahmed yacine et Nour elhouda".

Je dédie aussi ce mémoire A ma grande mère "Khadra" que dieu leur prête bonheur et longue vie.

A toute ma famille "Djeghoubbi" et ma famille "khalifa".

A tout mes amis "Bouthaina, Sidali, Fatiha, Wahiba, Mohamed, Djamel, Randa, Tidjani, Abdallah, Maissa, Hadjer, Aida, Chams elhouda, Salma, Marwa, Sabrine, Hania..."

A tous ceux qui me sont chères

A tous ceux que j'aime

Je dédie ce travail

Remerciement

Tout d'abord, je remercie dieu qui nous guident pour terminer ce travail humble.

J'exprime ma gratitude, mes remerciements a mes parents qui ont fait de leur mieux m'aider.

Je tiens a remercier vivement :

Mon encadreur Mr.Mohammed Laid Youmbai qui a proposé le thème de ce mémoire, pour ses conseils et ses dirigés dy début a la fin de ce travail.

Merci pour la qualité du sujet, merci pour vos conseils et la confiance que vous m'avais accorder au cours de cette année.

Je tiens a exprimer ma gratitude envers les membres de jury pour leurs disponibilités.

Mr.Mohamed Bousaid a l'université KASDI Merbah-Ouargla, pour avoir bien voulu me faire l'honneur d'accepter de présider le jury.

Mr.Med Amine Bahayou, Mr.Yassine Gerboussa et Mr.Med Tayeb Benmoussa a l'université de KASDI Merbah-Ouargla qui ont bien voulu faire partie de jury.

Mes remerciements vont bien entendu a toutes les personnes de département de mathématiques.

Je remercie aussi les personnes qi m'ont aidé et encouragé le long de ce travail.

Enfin, ces remerciements ne serait pas complétés sans mentionner mes parents, mes frères, mes amis.

Table des matières

Notations

- K : Corps.
- $\mathbb{Q}_p$: le corps de nombre p-adique.
- (X, d) : espace métrique.
- $(\tilde{X}, \tilde{d})$: espace métrique complet.
- C_x : l'ensemble de suite de Cauchy.
- $\widehat{\dot{x}}$: la classe d'équivalence.
- $\|$: valeur absolue sur K.
- $\|_\infty$: valeur absolue archimédienne.
- $\|_p$: valeur absolue p-adique.
- $\mathbb{Z}_p$: l'ensemble des entier p-adique.
- $\mathfrak{S}$: l'ensemble des suite de Cauchy dans $\mathbb{Q}, \|_p$.

INTRODUCTION

Soit $P(X,Y,Z) \in \mathbb{Z}[X,Y,Z]$ homogène, si $P(X,Y,Z) = 0$ possède des solutions non toutes nulles dans $\mathbb{Z}$ alors elle possède des solutions $\mod p^n$ pour tout p premier et tout $n \in N$. Pour montrer qu'elle n'a pas de solutions dans $\mathbb{Q}$ il suffit de montrer qu'elle n'a pas de solution $\mod p^n$ pour un p et un n.

Plus généralement pour une équation définie sur $\mathbb{Z}$ une première approche est de regarder si elle n'a pas de solution $\mod p$. Si elle en a des solutions $\mod p$ on étudiera l'équation $\mod p^2$, $\mod p^3$, $\mod p^4, \ldots$.

C'est pour traiter tous ces cas d'un seul coup que Hensel introduit les entiers p-adiques $\mathbb{Z}_p$. Un élément x de $\mathbb{Z}_p$ est une suite d'entier $(\alpha_k)_k$ tel que $0 \leq \alpha_k \leq p^k - 1$ et tel que $\forall k \geq 0, \alpha_{k+1} \equiv \alpha_k \ (p^k)$ c'est à dire

$$\mathbb{Z}_p = \lim_{\longleftarrow} \frac{\mathbb{Z}}{p^k\mathbb{Z}}$$

De même si le problème est posé sur $\mathbb{Q}$, on travaillera sur les nombres p-adiques $\mathbb{Q}_p = Frac(\mathbb{Z}_p)$.

Bien que définir $\mathbb{Q}_p$ comme étant le corps des fractions de $\mathbb{Z}_p$, et $\mathbb{Z}_p$ comme

étant la limite projective

$$\mathbb{Z}_p = \lim_{\longleftarrow} \frac{\mathbb{Z}}{p^k\mathbb{Z}}$$

associée à la projection

$$\frac{\mathbb{Z}}{p^{K+1}\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}^k}{p^K\mathbb{Z}}$$

soit plus facile et plus élégant, nous définirons nous plus pratiquement $\mathbb{Q}_p$ et $\mathbb{Z}_p$.

Ce mémoire se divise en trois chapitres. Dans le premier chapitre, nous présentons la complétion d'un espace métrique en général.

Dans le deuxième chapitre nous exposons les valeurs absolues sur un corps en général et insistons sur la valeur absolue non archimédienne sur le corps des rationnels $\mathbb{Q}$.
Nous complétons alors $\mathbb{Q}, \|_p$ pour obtenir $\mathbb{Q}_p$ et nous nous familiarisons enfin avec les nombres p-adiques.

le dernier chapitre présente le principe de Hasse ou principe Local-Global et montre son obstruction dans les cas des cubiques non singulières.

Chapitre 1

Complété d'un Espace métrique

1.1 Espace métrique

Définition 1.1.1 *Soit E un ensemble (non vide). On appelle distance sur E une application $d : E \times E \longrightarrow \mathbb{R}$ vérifiant les trois propriétés suivantes :*

1. $d(x, y) = 0 \Leftrightarrow x = y \quad \forall x, y \in E.$
2. $d(x, y) = d(y, x) \quad \forall x, y \in E$ *(symétrie).*
3. $d(x, y) \leq d(x, z) + d(z, y) \quad \forall x, y, z \in E$ *(inégalité triangulaire).*

Si d est une distance sur E on dit que (E, d) est un espace métrique.

Exemple 1.1.2 *1/ $\mathbb{R}$ et la valeur absolue : $d(x, y) = |x - y|$.*

2/ $\mathbb{R}^n$ (ou $\mathbb{C}^n$) et la distance euclidienne $d(x, y) = (\sum |x_i - y_i|^2)^{\frac{1}{2}}$.

3/ $\mathbb{R}^n$ (ou $\mathbb{C}^n$) munis de $d_1(x, y) = \sum |x_i - y_i|$ ou encore de

$$d_\infty(x, y) = \sup_{1 \leq i \leq n} |x_i - y_i|.$$

1.2 Espaces métriques complets

1.2.1 Suite de Cauchy

Définition 1.2.1 *on dit qu'une suite $(x_n)_{n\in N}$ d'un espace métrique (X,d) est de Cauchy si elle vérifie*

$$\forall \varepsilon > 0, \exists N_\varepsilon \in \mathbb{N}, \forall m,n \geq N_\varepsilon, d(x_m,x_n) \leq \varepsilon.$$

Proposition 1.2.2 *Une suite de Cauchy est toujours bornée.*

Preuve.

Il existe N_1 tel que

$$\forall m,n \geq N_1,\ d(x_m,x_n) \leq 1.$$

En particulier on a pour $n \geq N_1, d(x_n,x_{N_1}) \leq 1$ et en posant

$$M = \max_{K\leq N_1} d(x_K,x_{N_1}).$$

$$\forall n \in \mathbb{N}, d(x_n,x_{N_1}) \leq \max\{M,1\}.$$

■

Proposition 1.2.3 *Toute suite convergente est de Cauchy.*

Preuve.

Soit $(x_n)_{n\in N}$ un suite de (X,d) tel que

$$\lim_{k\longrightarrow\infty} x_{n_k} = l \in X.$$

Pour $\varepsilon > 0$ il existe $N_\varepsilon \in \mathbb{N}$ tel que

$$d(x_n,l) \leq \frac{\varepsilon}{2}.$$

Pour $n \geq N_\varepsilon$. On a alors

$$\forall m,n \geq N_\varepsilon, d(x_m,x_n) \leq d(x_m,l) + d(l,x_n) \leq \varepsilon$$

et la suite est de Cauchy. ■

1.3 Complété d'un espace métrique

Définition 1.3.1 *On dit que l'espace métrique (X, d) est* ***complet*** *si toute suite de Cauchy converge.*

Exemple 1.3.2 *1. $\mathbb{R}$ est complet*

soit $(x_n)_{n\in\mathbb{N}}$ une suite de Cauchy de $\mathbb{R}$. Elle est bornée $\forall n \in \mathbb{N}, |x_n| \leq M$. On peut donc extraire une sous-suite qui converge dans R (puisque $[-M, M]$ est compact). Mais alors la Proposition 1.2.3 donne la convergence de toute la suite.

2. $\mathbb{Q}$ n'est pas complet On peut approcher un irrationnel $r \in \mathbb{R} \setminus \mathbb{Q}$ par une suite de rationnels $x_n = \frac{p_n}{q_n}$. La suite $(x_n)_{n\in\mathbb{N}}$ est de Cauchy dans $\mathbb{R}$ et donc dans $\mathbb{Q}$. Elle ne converge pas dans $\mathbb{Q}$ puisque $r \notin \mathbb{Q}$.

Théorème 1.3.3 *Si (X, d) est un espace métrique, il existe un espace métrique $(\tilde{X}, \tilde{d})$ complet dont (X, d) est un sous-espace dense. Cet espace est unique à isométrie près. On l'appelle* ***le complété*** *de (X, d).*

Preuve.

1. **Unicité :** Supposons que (X, d) soit un sous-espace dense de deux espaces métriques $(\tilde{X}_1, \tilde{d}_1)(\tilde{X}_2, \tilde{d}_2)$ dont les distances d_1 et d_2 prolongent d. Le plongement $i_2 : (X, d) \longrightarrow (\tilde{X}_2, \tilde{d}_2)$ est une isométrie. En particulier elle est uniformément continue tandis que X est dense dans $(\tilde{X}_1, \tilde{d}_1)$ et tandis que $(\tilde{X}_2, \tilde{d}_2)$ est complet. Elle se prolonge donc de façon unique en une isométrie de $i_2 : (\tilde{X}_1, \tilde{d}_1) \longrightarrow (\tilde{X}_2, \tilde{d}_2)$. De même l'isométrie $i_1 : (X, d) \longrightarrow (\tilde{X}_1, \tilde{d}_1)$ a un unique prolongement isométrique i_1 de $\tilde{X}_2$ dans $\tilde{X}_1$. Enfin comme $\tilde{i_1} \circ \tilde{i_2}|_X = Id_X$, on a par unicité du prolongement continu $\tilde{i_1} \circ \tilde{i_2} = Id_{\tilde{X}_1}$, L'isométrie $\tilde{i}_1$ est surjective donc une bijection isométrique de $\tilde{X}_2$ sur $\tilde{X}_1$. Les espaces $(\tilde{X}_1, \tilde{d}_1)$ et $(\tilde{X}_2, \tilde{d}_2)$ sont isométriques.

2. **Existence :** On considère C_X l'ensemble des suites de Cauchy de (X, d).
   Si $x = (x_n)_{n\in\mathbb{N}}$ et $y = (y_n)_{n\in\mathbb{N}}$ sont deux suites de Cauchy de X alors l'écart

$$|d(x_n, y_n) - d(x_m, y_m)| \leq |d(x_n, y_n) - d(x_n, y_m)| + |d(x_n, y_m) - d(x_m, y_m)|$$

$$\leq d(y_n, y_m) + d(x_n, x_m)$$

est plus petit que $\varepsilon > 0$ pour $m, n \geq N_\varepsilon$ avec N_ε assez grand puisque x et y sont deux suites de Cauchy.

Ainsi la suite $(d(x_n, y_n))_{n\in\mathbb{N}}$ est de Cauchy dans $\mathbb{R}$ et donc converge. On pose alors

$$\forall x, y \in C_X, \delta(x, y) = \lim_{n\longrightarrow\infty} d(x_n, y_n).$$

Par passage à la limite, on a pour tout $x, y, z \in C_X$

$$\delta(y, x) = \delta(x, y) \text{ et } \delta(x, z) \leq \delta(x, y) + \delta(y, z).$$

Afin de définir une distance à partir de δ, on met sur C_X la relation d'équivalence

$$(x\mathcal{R}y) \Leftrightarrow (\delta(x, y) = 0) \Leftrightarrow (\lim_{n\longrightarrow\infty} d(x_n, y_n) = 0)$$

et on prend pour $\tilde{X}$ l'ensemble quotient $C_X/\mathcal{R}$ et pour $\tilde{d}$ la fonction

$$\begin{aligned} \tilde{d} : \tilde{X} \times \tilde{X} &\to \mathbb{R}_+ \\ (\dot{\widehat{x}}, \dot{\widehat{y}}) &\to \tilde{d}(\dot{\widehat{x}}, \dot{\widehat{y}}) = \delta(x, y). \end{aligned}$$

La quantité $\delta(x, y)$ ne dépend pas du choix de x dans la classe d'équivalence $\dot{\widehat{x}}$ et du choix de y dans sa classe $\dot{\widehat{y}}$ grâce à l'inégalité triangulaire. Il reste à vérifier que $(\tilde{X}, \tilde{d})$ est un espace métrique complet dans lequel X est inclus et dense.

a) $\tilde{d}$ est une distance sur $\tilde{X}$. La symétrie et l'inégalité triangulaire sont héritées de δ et l'équivalence $(\tilde{d}(\dot{\widehat{x}}, \dot{\widehat{y}}) = 0) \Leftrightarrow (\dot{\widehat{x}} = \dot{\widehat{y}})$ vient du passage au quotient.

b) $X \subset \tilde{X}$: Pour $a \in X$ on considère la suite constante $x[a] = (x_n = a)_{n\in\mathbb{N}}$ qui est un élément de C_X et on identifie a et $\dot{\widehat{x}}[a]$ De plus le plongement de (X, d) dans $(\tilde{X}, \tilde{d})$ est isométrique puisque $\tilde{d}(\dot{\widehat{x}}[a], \dot{\widehat{x}}[b]) = \delta(x[a], x[b]) = d(a, b)$.

c) Soit $(\dot{\widehat{x^n}})_{n\in\mathbb{N}}$ une suite de Cauchy de $(\tilde{X}, \tilde{d})$ En prenant des représentants cela revient à considérer une suite $(x^n)_{n\in\mathbb{N}}$ de C_X telle que

$$\forall \varepsilon > 0, \exists N_\varepsilon \in \mathbb{N}, \forall m, r \geq N_\varepsilon, \delta(x^m, x^n) \leq \varepsilon.$$

i) pour $n \in \mathbb{N}$ fixé $x^n = (k_k^n)_{k\in\mathbb{N}}$ est une suite de Cauchy de X et il existe $k_n \in \mathbb{N}$ tel que : $\forall k, k' \geq k_n, d(x_k^n, x_{k'}^n) \leq \frac{1}{n+1}$. Procédé diagonal : On considère la suite $x = (x_{k_n}^n)_{n\in\mathbb{N}}$ de X.

ii) $x \in C_X$: Pour $m, n, k \in \mathbb{N}$, on écrit

$$d(x_n, x_m) = d(x_{k_n}^n, x_{k_m}^m) \leq d(x_{k_n}^n, x_k^n) + d(x_k^n, x_k^m) + d(x_k^m, x_{k_m}^m)$$

et en prenant $k \geq \max\{k_n, k_m\}$,

$$d(x_n, x_m) \leq \frac{1}{n+1} + \frac{1}{m+1} + d(x_k^n, x_k^m).$$

complété.

Pour $\varepsilon > 0$ il existe N_ε tel que $\delta(x^n, x^m) \leq \frac{\varepsilon}{4}$ pour $m, n \geq N_\varepsilon$. Pour de tels m et n on a alors par définition de $\delta, d(x_k^n, x_k^m) \leq \frac{\varepsilon}{2}$ pour k assez grand. Ainsi, on obtient

$$d(x_n, x_m) \leq \frac{1}{n+1} + \frac{1}{m+1} + \frac{\varepsilon}{2}.$$

et on peut trouver $N'_\varepsilon \in \mathbb{N}$ tel que $d(x_n, x_m) \leq \varepsilon$ pour $m, n \geq N'_\varepsilon$.

iii) $\dot{\widehat{x}} = \lim_{n\to\infty} \dot{\widehat{x^n}}$: Il suffit de montrer $\lim_{n\to\infty} \delta(x^n, x) = 0$. Pour $n, j \in \mathbb{N}$ on a

$$d(x_j^n, x_j) \leq d(x_j^n, x_n) + d(x_n, x_j) = d(x_j^n, x_{k_n}^n) + d(x_n, x_j).$$

Soit $\varepsilon > 0$, avec les notations précédentes,

on a pour $n \geq N'_\varepsilon$ et $j \geq \max\{k_n, N'_\varepsilon\}$

$$d(x_j^n, x_j) \leq \frac{1}{n+1} + \varepsilon.$$

En prenant la limite quand $j \to \infty$ on obtient

$$\forall n \geq N'_\varepsilon, \delta(x^n, x) = \lim_{j\to\infty} d(x_j^n, x_j) \leq \frac{1}{n+1} + \varepsilon.$$

Et en prenant $n \geq N''_\varepsilon$ avec N''_ε assez grand cela donne $\delta(x^n, x) \leq 2\varepsilon$.

d) X est dense dans $(\tilde{X}, \tilde{d})$. Si $\dot{\widehat{x}}$ est un élément quelconque de $\tilde{X}$, on prend un représentant $x = (x_n)_{n\in\mathbb{N}}$ dans C_X et on considère la suite de suites constantes $(x[x_n])_{n\in\mathbb{N}}$ (la classe de la suite constante $x[a] \in C_X$ s'identifiant avec l'élément a de X).

On a alors

$$\delta(x[x_n], x) = \lim_{k\to\infty} d(x_n, x_k) \leq \varepsilon \text{ pour tout } \varepsilon > 0 \text{ et } n \geq N_\varepsilon.$$

On a donc

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} \dot{\widehat{x}}[x_n] = \dot{\widehat{x}}$$

dans $(\tilde{X}, \tilde{d})$.

■

Chapitre 2

Les Complétés de $\mathbb{Q}$

2.1 Valeurs absolues de $\mathbb{Q}$

Définition 2.1.1 *Soit k un corps.On appelle valeur absolue sur k toute application $\|$ de k dans $\mathbb{R}_+$ telle que :*

$$\forall x \in k, |x| = 0 \Leftrightarrow x = 0 \tag{2.1}$$

$$\forall x, y \in k, |xy| = |x||y| \tag{2.2}$$

$$\forall x, y \in k, |x + y| \leqslant |x| + |y| \tag{2.3}$$

Un corps muni d'une valeur absolue s'appelle un corps valué.

L'égalité (2.2) et (2.1) montre que $|1| = 1 \quad (x = y = 1)$, $| - 1| = 1 \quad (x = y = -1)$ puisque $|\frac{1}{x}| = \frac{1}{|x|}$.

Exemple 2.1.2 *1. la valeur absolue triviale est définie par*

$$|x| = \begin{cases} 0 & si\ x = 0 \\ 1 & sinon \end{cases}$$

2. *L'application de $\mathbb{Q}$ sur $\mathbb{R}_+$ définie par*

$$|x| = Max\{x, -x\}$$

est une valeur absolue sur $\mathbb{Q}$, on l'appelle valeur absolue archimédienne de $\mathbb{Q}$ et on la note $\|_\infty$.

3. *Soit p un nombre premier. On considère la fonction $\|_p$ définie par*

$$\forall x \in \mathbb{Q}^\times, |x|_p = p^{-k} \text{ si } x = p^k \frac{a}{b} \text{ avec } (a,p) = (b,p) = 1 \text{ et } |0|_p = 0,$$

où (a, b) désigne le pgcd de a et de b.

On l'appelle valeur absolue p-adique de $\mathbb{Q}$.

Lemme 2.1.3 *L'application $x \longrightarrow |x|_p$ est une valeur absolue sur $\mathbb{Q}$ .Elle vérifie, en outre, l'inégalité (ultramétrique)*

$$\forall x, y \in \mathbb{Q}, |x+y|_p \leqslant max(|x|_p, |y|_p). \tag{2.4}$$

Cette valeur absolue $\|_p$ est appelée valeur absolue p-adique de $\mathbb{Q}$.

Preuve.

Par définition de $\|_p$, l'égalité (2.1) est satisfaite.

Si $x = p^k \frac{a}{b}$ et $y = p^{k'} \frac{c}{d}$ avec $(a,p) = (b,p) = (c,p) = (d,p) = 1$

alors

$$xy = p^{k+k'} \frac{ac}{bd}$$

ce qui nou donne

$$|xy|_p = p^{-(k+k')} = p^{-k} p^{-k'} = |x|_p |y|_p.$$

et démontre légalité (2.2).

D'autre part, en supposant que $k \leqslant k'$ (si non on échange x et y), on a

$$|y|_p = \max(|x|_p, |y|_p),$$

et

$$x+y=p^k(\frac{a}{b}+p^{k'-k}\frac{c}{d})=p^k(\frac{ad+cbp^{k'-k}}{bd}).$$

Puisque $ad+cbp^{k'-k}$ est un entier, il existe deux entiers r et a' tels que

$$ad+cbp^{k'-k}=p^r a' \text{ avec } (a',p)=1 \text{ et } r\geqslant 0.$$

En outre, p est premier à b et d donc p est premier à bd, ce qui nous donne l'inégalité

$$|x+y|_p=p^{-(k+r)}\leqslant p^{-k}=\max(|x|_p,|y|_p)\leqslant |x|_p+|y|_p.$$

Qui démontre les inégalités (2.3) et (2.4). ■

Remarque 2.1.4 *Il est de notoriété publique que l'ensemble des entiers relatifs $\mathbb{Z}$ est un ensemble non borné pour la distance usuelle sur $\mathbb{R}$ induit par la valeur absolue archimédienne $\|_\infty$. Par contre, si p désigne un nombre premier, tout entier n s'écrit sous la forme $p^r m$ ou r est un entier positif et m' un entier relatif premier à p donc*

$$\forall n\in z, |n|_p=p^{-r}\leqslant 1.$$

ce qui implique que l'ensemble $\mathbb{Z}$ est borné pour toute valeur absolue p-adique $\|_p$.

Exemple 2.1.5 *Nous savons que la valeur absolue triviale*

$$x\mapsto |x|=\begin{cases} 0 \text{ si } x=0 \\ \text{et } 1 \text{ sinon}\end{cases}$$

induit la distance triviale

$$(x,y)\mapsto d(x,y)=\begin{cases} 0 \text{ si } x=y \\ \text{et } 1 \text{ sinon}\end{cases}$$

Nous savons aussi que la valeur absolue usuelle induit sur $\mathbb{Q}$ la distance usuelle

$$(x,y)\mapsto d_\infty(x,y)=|x-y|_\infty.$$

Définition 2.1.6

- *On appelle corps value, tout couple de la forme $(k,\|)$ ou k est un corps et $\|$ est une valeur absolue sur k.*

- *On appelle distance induite sur k par $\|$, la distance $d_{\|}$ sur k définie par*

$$\forall x, y \in k, d_{\|}(x, y) = |x - y|$$

- *On dit que deux valeurs absolues sur k, $\|_1$ et $\|_2$, sont équivalentes ssi leurs distances associées respectives induisent la même topologie sur k.*

Rappelons que deux distances d_1 et d_2 sur un espace métrique X définissent la même topologie si les ouverts pour la distance d_1 sont les ouverts pour la distance d_2.

Lemme 2.1.7 *Soit k un corps et $\|_1, \|_2$ deux valeurs absolues sur k.*

Les valeurs absolues $\|_1$ et $\|_2$ sont équivalentes si et seulement si pour toute suite $(x_n)_{n\in\mathbb{N}}$ de k

$$(|x_n|_{1\,n\longrightarrow+\infty} \longrightarrow 0) \Leftrightarrow (|x_n|_{2\,n\longrightarrow+\infty} \longrightarrow 0).$$

Preuve.

$\Longrightarrow$ Supposons que les valeurs absolues $\|_1$ et $\|_2$ sont équivalentes.

Soit $(x_n)_n \geqslant 0$ une suite de k convergent vers 0 pour la distance d_1. Alors, pour tout ouvert V de 0 (pour la distance d_1), il existe un rang n_0 tel que $\forall n \geqslant n_0$, $u_n \in V$.Or tout ouvert pour d_2 est un ouvert de d_1, donc pour tout ouvert V de 0 (pour la distance d_2), il existe un rang n_0 tel que $\forall n \geqslant n_0$, $u_n \in V$ ce qui démontre que $(x_n)_n \geqslant 0$ converge vers 0 pour la distance d_2.

$\Longleftarrow$ Supposons que pour toute suite $(x_n)_n \geqslant 0$ de k $(x_n)_{n\in\mathbb{N}}$ de k

$$(|x_n|_{1\,n\longrightarrow+\infty} \longrightarrow 0) \Leftrightarrow (|x_n|_{2\,n\longrightarrow+\infty} \longrightarrow 0).$$

Démontrer que les ouverts pour d_1 sont les ouverts pour d_2 revient à démontrer que les fermés pour d_1 sont les fermés de d_2 (le complémentaire d'un ouvert est un fermé et vice-versa). La caractérisation séquentielle des fermés montre que F est fermé si et seulement si pour toute suite $(x_n)_n \geqslant 0$ d'éléments de F convergente vers x dans k pour la distance d_1 alors $x \in F$.

Soit F un fermé pour la distance d_1 et soit $(x_n)_n \geqslant 0$ une suite d'éléments de F convergent vers $x \in K$ pour la distance d_2. Alors

$$d_{\|_2}(x_n, x) = |x_n - x|_2 \longrightarrow 0 \Longleftrightarrow |x_n - x|_1 = d_{\|_1}(x_n, x) \longrightarrow 0.$$

On en déduit que la suite $(x_n)_n \geqslant 0$ converge vers x dans k pour la distance d_1 et puisque F est fermé pour la distance d_1, $x \in F$. L'ensemble F est donc fermé pour la distance d_2. En échangeant les rôles de d_1 et d_2, on conclut.

■

Théorème 2.1.8 *Soient $\|_1$ et $\|_2$ deux valeurs absolus sur k, alors $\|_1$ et $\|_2$, sont équivalente si et seulement si il existe un réel positif a tel que*

$$\forall x \in k, \qquad |x|_1 = |x|_2^a.$$

Preuve.

L'implication réciproque est évidente grâce au lemme 2.1.7

Pour l'implication directe, soit x un élément de k tel que $|x|_1 < 1$.

La suite $(x_n)_{n\in\mathbb{N}}$ converge vers 0 ($|x^n|_1 = |x|_1^n$) dans $(k, d_{\|_1})$ donc elle converge vers 0 dans $(k, d_{\|_2})$ c'est-à-dire $|x|_2^n = |x^n|_2 \longrightarrow_{n\longrightarrow+\infty} 0$, d'où $|x|_2 < 1$.

En échangeant le rôle joué par les deux valeurs absolues, on obtient que

$$\forall x \in k, (|x|_1 > 1) \Longleftrightarrow (|x|_2 > 1),$$

ensuite en remplaçant x par $\dfrac{1}{x}$ $(x \neq 0)$, on obtient

$$\forall x \in k, (|x|_1 < 1) \Longleftrightarrow (|x|_2 < 1).$$

et par conséquent

$$\forall x \in k, (|x|_1 = 1) \Longleftrightarrow (|x|_2 = 1).$$

Ainsi si $\|_1$ est la valeur absolue triviale, on en déduit que $\|_2$ est également la valeur triviale.

Supposons $\|_1$ ne soit pas triviale, il existe $x_0 \in k$ tel que $|x_0|_1 > 1$
(donc $|x_0|_2 > 1$) ce qui implique qu'il existe $a \in \mathbb{R}_+$ tel que $|x_0|_1 = |x_0|_2^a$
($a = \frac{ln|x_0|_1}{ln|x_0|_2} > 0$). Soit $x \in k$ tel que $|x|_1 > 1$. Considérons le réel b pour lequel $|x|_1 = |x_0|_1^b$.

Pour tout rationnel $\frac{p}{q} < b$, on a les équivalences suivantes :

$$|x|_1 < |x_0|_1^{\frac{p}{q}} \Longleftrightarrow |x^q|_1 < |x_0^p|_1 \Longleftrightarrow |\frac{x^q}{x_0^p}|_1 < 1 \Longleftrightarrow |x^q|_2 < |x_0^p|_2 \Longleftrightarrow |x|_2 < |x_0|_2^{\frac{p}{q}}.$$

En faisant tendre $\frac{p}{q}$ vers b dans $\mathbb{R}$, on obtient que $|x|_2 \leqslant |x_0|_2^b$.
En appliquant le même raisonnement à un rationnel $\frac{p}{q} > b$ puis en passant à la limite, on obtient que $|x|_2 \geqslant |x_0|_2^b$. Ce qui nous fournit l'égalité

$$|x|_2 = |x_0|_2^b = |x_0|_1^{\frac{b}{a}} = |x|_1^{\frac{1}{a}} \Longrightarrow |x_1| = |x|_2^a,$$

valable pour tout élément x de k tel que $|x_1| > 1$.
En remplaçant x par $\frac{1}{x}$ et en utilisant la multiplicativité des valeurs absolues, on en déduit que

$$\forall x \in k, \text{ telle que } |x_1| \neq 1, |x|_1 = |x|_2^a.$$

Soit $x \in k$ tel que $|x|_1 = 1$. L'élément $\frac{x}{x_0}$ qui vérifie

$$|\frac{x}{x_0}|_1 = \frac{|x|_1}{|x_0|_1} = \frac{1}{|x_0|_1} < 1,$$

donc on a

$$|\frac{x}{x_0}|_1 = |\frac{x}{x_0}|_2^a \Longleftrightarrow |x|_1 = |x|_2^a \qquad (\text{car } |x_0|_1 = |x_0|_2^a),$$

ce qui nous permet d'affirmer

$$\forall x \in k, \qquad |x|_1 = |x|_2^a.$$

■

Corollaire 2.1.9 *Deux valeurs absolues $\|_p$ et $\|_l$ sont équivalentes si et seulement si $p = l$.*

Preuve.

La réciproque est triviale. Pour l'implication directe, il suffit de considérer la suite (p^n) $n \geqslant 0$.

Elle converge vers 0 pour $\|_p$ car $|p^n|_p = p^{-n} \longrightarrow 0$ quand $n \longrightarrow +\infty$ et si $p \neq l$, elle ne converge pas vers 0 pour $\|_l$ car $|p^n|_l = 1 \nrightarrow 0$. ■

Théorème 2.1.10 *(D'ostrowski) Toute valeur absolue sur $\mathbb{Q}$ est équivalente à l'un des valeur absolue suivantes :*

- *la valeur absolue triviale.*
- *La valeur absolue archimédienne $\|_\infty$.*
- *à une certaine valeur absolue p-adique $\|_p$.*

Preuve.

Soit $\|$ une valeur absolue sur $\mathbb{Q}$ non triviale.

1. Cas où $\mathbb{Z}$ est un ensemble borné pour $\|$.
   Pour tout $n \in \mathbb{Z}\backslash\{0\}$, la suite $(n^k)_{k\geqslant 0}$ est bornée donc la suite $(|n^k| = |n|^k)_k$ l'est également, ce qui démontre que

   $$\forall x \in \mathbb{Z}, |n| \leqslant 1. \tag{2.5}$$

   La valeur absolue $\|$ n'est pas triviale. Il existe alors un nombre entier non nul n' tel que $|n'| < 1$ (sinon pour tout entier non nul n, l'égalité $|n| = 1$ est vérifiée donc pour tout rationnel $\frac{a}{b}$, on a $|\frac{a}{b}| = 1$, ce qui contredit l'hypothèse).
   Pour ce nombre n', il existe des nombres premiers $p_1, \ldots, p_r$ deux à deux distincts et des entiers positifs $l_1, \ldots, l_r$ tels que $n' = \pm p_1^{l_1} \ldots p_r^{l_r}$ donc $|p_1|^{l_1} \ldots |p_r|^{l_r} = |n'| < 1$. Chacun des facteurs de ce produit est inférieur à 1 et le produit est strictement plus petit que 1 donc il existe un nombre premier p_i tel que $|p_i| < 1$. Désormais, nous noterons p le nombre premier p_i.

   Le théorème de Bezout montre que pour tout nombre n premier à p, il existe des entiers relatifs a_k et b_k tels que $a_k p^k + b_k n^k = 1$.

Supposons que $|n| < 1$ alors

$$|a_k p^k| = |a_k||p|^k \leqslant |p^k|_{k\longrightarrow+\infty} \longrightarrow 0,$$

et

$$|b_k n^k| = |b_k||n|^k \leqslant |n|^k_{k\longrightarrow+\infty} \longrightarrow 0.$$

On en déduit que

$$\forall k \in \mathbb{N} \ \ , 1 = |1| = |a_k p^k + b_k n^k| \leqslant |a_k p^k| + |b_k n^k|_{k\longrightarrow+\infty} \longrightarrow 0,$$

ce qui est absurde (on remarquera que dans l'inégalité précédente $\|$ désigne notre valeur absolue et non la valeur absolue archimédienne qui est notée $\|_\infty$).

Ainsi pour tout nombre n premier à p, on a $|n| = 1$. Tout nombre rationnel non nul x s'écrit sous la forme $x = p^k \dfrac{a}{b}$ avec $(a, p) = (b, p) = 1$ donc

$$\forall x \in \mathbb{Q}, \quad |x| = |p|^k = p^{-ka} = |p^k|^a_p = |x|^a_p \ \text{ avec } \ a = -\frac{ln|p|}{lnp} > 0.$$

Ainsi si $\mathbb{Z}$ est un ensemble borné pour $\|$, alors $\|$ est équivalente à une certaine valeur p-adique.

2. Cas ou $\mathbb{Z}$ est un ensemble non borné pour $\|$.

   Soit a un entier non nul positif tel que $|a| \neq 1$ (donc $a \notin \{0, 1\} \Longrightarrow a > 1$).

   Tout entier naturel n s'écrit dans la base a sous la forme

$$n = \sum_{m=0}^{r_n} q_m a^m \ \text{ avec } \ k_m \in \{0, ..., a-1\}, q_{r_n} \neq 0.$$

   et

$$r_n \leqslant \frac{\ln n}{\ln a} \ \ (\text{car } \ a^{r_n} \leqslant n_{r_n} a^{r_n} \leqslant n).$$

   Si l'on pose

$$M = \max_{s\in\{0,...,a-1\}}(|s|),$$

   il est immédiat que

$$|n| \leqslant M\Sigma_{m=0}^{r_n}|a|^m.$$

D'autre part, pour tout entier k, l'entier n^k peut s'écrire

$$n^k = \sum_{m=0}^{r_n k} q'_m a^m \text{ avec } r_n k \leqslant \frac{\ln n^k}{\ln a} = k\frac{\ln n}{\ln a},$$

ce qui nous fournit l'inégalité

$$\forall k \in \mathbb{N}, |n|^k = |n^k| \leqslant M \sum_{k=0}^{r_n k} |a|^k \tag{2.6}$$

Supposons qu'il existe un entier $a > 1$ tel que $|a| \leqslant 1$. alors l'inégalité (2.6) montre que

$$\forall n \in \mathbb{N}, \forall k \geqslant 0, |n|^k \leqslant M(r_{n^k} + 1) \leqslant M(k\frac{\ln n}{\ln a} + 1) \Longrightarrow |n| \leqslant M^{\frac{1}{k}}(k\frac{\ln n}{\ln a} + 1)^{\frac{1}{k}}.$$

Puisque

$$\frac{1}{k}\ln(k\frac{\ln n}{\ln a} + 1)_{k\overset{\sim}{\longrightarrow}+\infty}\frac{1}{k}ln(k\frac{\ln n}{\ln a})_{k\longrightarrow+\infty} \longrightarrow 0,$$

en faisant tendre k vers $+\infty$ dans l'inégalité précédente,on obtient que

$$\forall n \in \mathbb{N}, |n| \leqslant 1,$$

l'ensemble $\mathbb{N}$ donc $\mathbb{Z}$ est bornée pour $\|$ ce qui est absurde.

Ainsi pour tout entier naturel $a > 1$, on a $|a| > 1$. Nous reprenons l'inégalité (2.6) pour un entier $a > 1$ (donc $|a| > 1$ ce qui nous donne

$$\forall n \in \mathbb{N}, \forall k \geqslant 0, |n| \leqslant M^{\frac{1}{k}}(\frac{|a|^{r_n+1} - 1}{|a| - 1})^{\frac{1}{k}} = (\frac{M}{1 - |a|})^{\frac{1}{k}}(|a|^{k\frac{\ln n}{\ln a}+1} - 1)^{\frac{1}{k}}.$$

La suite $(|a|^{k\frac{\ln n}{\ln a}+1})_k$ tend vers $+\infty$ lorsque $k \longrightarrow +\infty$ donc

$$\frac{1}{k}\ln(|a|^{k\frac{\ln n}{\ln a}+1} - 1) = \frac{1}{k}[\underbrace{ln(|a|^{k\frac{\ln n}{\ln a}+1})}_{\longrightarrow+\infty} + ln(1 - \underbrace{|a|^{-(k\frac{\ln n}{\ln a}+1)})}_{\longrightarrow 0}]_{k\overset{\sim}{\longrightarrow}+\infty} -$$
$$\frac{1}{k}\ln(|a|^{k\frac{\ln n}{\ln a}+1})_{k\overset{\sim}{\longrightarrow}+\infty}\frac{k\frac{\ln n}{\ln a}}{k}\ln|a|_{k\overset{\longrightarrow}{\longrightarrow}+\infty}\frac{\ln n}{\ln a}.$$

En faisant tendre $k \longrightarrow +\infty$ dans l'inégalité ci-dessus

$$\forall a \in \mathbb{N} \text{ tel que } a > 1, \quad \forall n \in \mathbb{N}^{\times}, |n| \leqslant |a|^{\frac{\ln n}{\ln a}} \Longleftrightarrow \frac{\ln |n|}{\ln n} \leqslant \frac{\ln |a|}{\ln a}.$$

Si l'on échange le rôle de a et de n dans l'inéquation précédente, on obtient que le rapport $\dfrac{\ln |n|}{\ln n}$ est constant sur les entiers strictement plus grand que 1. Désignons par d cette constante : alors pour tout entier naturel $n > 1$, $|n| = n^d$, la formule étant trivialement vérifiée pour $n = 0$ et $n = 1$. On peut étendre par multiplicativité cette formule aux entiers relatifs ($|-1| = 1$) puis à l'ensemble des rationnels.

On peut remarquer que le réel $d \in]0, 1]$ est positif ($d = \dfrac{\overbrace{\ln |a|}^{>0}}{\underbrace{\ln a}_{>0}}$ pour tout entier $a > 1$) et plus petit que 1

($|a| = |\underbrace{1 + 1 + \cdots + 1}_{a \text{ fois}}| \leqslant |a|_{\infty}|1| = a$).

Ainsi, si $\mathbb{Z}$ est un ensemble non borné pour $\|$, alors $\|$ est équivalente à la valeur absolue archimédienne $\|_{\infty}$.

■

Définition 2.1.11 *Une valeur absolue sur $\mathbb{Q}$ est dite :*

- *archimédienne si et seulement si elle est équivalente à la valeur absolue $\|_{\infty}$.*
- *non archimédienne si et seulement si elle est équivalente à une certaine valeur absolue p-adique.*

2.2 Complétion

Définition 2.2.1 *Un corps K est complet par rapport à la valeur absolue $\|$ si toute suite de Cauchy dans K est convergente.*

Définition 2.2.2 *On dit qu'un corps value $K, \|\|$ est le complété d'un corps value $k, \|$ si :*

i) $K, \|\|$ est complet.

ii) Il existe une injection $\lambda : k \longrightarrow K$ qui préserve la valeur absolue i.e

$$\|\lambda(x)\| = |x|, \forall x \in k.$$

iii) K est l'adhérence de $\lambda(k)$ par rapport à la topologie induite par. $\|\|$

Le complété d'un corps k existe toujours et est unique à isomorphisme prés, on identifie en générale k et $\lambda(k)$, $\|$ et $\|\|$ de sorte que k soit va comme sous corps de K.

2.3 Complété de $\mathbb{Q}, \|_p$

soit $\mathfrak{S}$ l'ensemble des suite de Cauchy dans $\mathbb{Q}, \|_p$, $\mathfrak{S}$ est un anneau pour les opérations

$$\{a_n\} + \{b_n\} = \{a_n + b_n\} \quad \{a_n\}\{b_n\} = \{a_n b_n\}.$$

soit $\mathfrak{N}$ le sous ensemble de $\mathfrak{S}$ formé des suites qui tendent vers 0.

$\mathfrak{N}$ est un idéal maximal de $\mathfrak{S}$ de sorte que $\dfrac{\mathfrak{S}}{\mathfrak{N}}$ soit un corps, il sera note $\mathbb{Q}_p$.
Définition de la valeur absolue sue $\mathfrak{S}$

$$\|\{a_n\}\|_p = 0 \text{ si } \{a_n\} \in \mathfrak{N}$$

sinon

$$\{a_n\} \in \mathfrak{S}_1, \{a_n\} \notin \mathfrak{N}$$

alors

$$\exists N \in \mathbb{N}, \quad n > N \Longrightarrow |a_n - a_N|_p < |a_n|$$

donc

$$|a_n|_p = |a_N|_p$$

posons $|\{a_n\}|_p = |a_N|_p$

Montrons que $\mathfrak{N}$, est maximal

soit $\mathfrak{M} \supsetneq \mathfrak{N}$ un idéal de $\mathfrak{S}, \mathfrak{M}$ contient un élément $\{a_n\} \notin \mathfrak{N}, \{a_n\} \in \mathfrak{S}$, il existe donc un nombre fini de a_n qui peuvent être nul. Donc en remplaçant les 0 par 1 on obtient un élément n'appartenant par $\mathfrak{N}$ et appartenant à $\mathfrak{M}$

On peut donc supposer que tous les a_n sont non nul donc

$$\{a_n^{-1}\} \in \mathfrak{S} \text{ et } \{a_n^{-1}\}\{a_n\} \in \mathfrak{M} \Longrightarrow \mathfrak{M} = \mathfrak{S},$$

d'où $\mathfrak{N}$ maximal et $\dfrac{\mathfrak{S}}{\mathfrak{N}}$ corps.
Soit l'application :

$$\mathbb{Q} \to \mathfrak{S}$$

$$a \mapsto \{a\}$$

la fonction $|\{a_n\}|$ sur $\mathfrak{S}$ induit une fonction sur $\mathfrak{S}/\mathfrak{N}$ qui une valeur absolue et qui coïncide avec $\|_p$ sur $\mathbb{Q}$:$|\overline{\{a\}}\|_p = |a|_p$

Enfin on peut voir que $\mathfrak{S}/\mathfrak{N}$ est complet.

Exemple 2.3.1

- $\mathbb{Q}$ *munie de la valeur absolue triviale est complet.*
- $\mathbb{Q}, \|_\infty$ *n'est pas complet, la suite* $x_n = \sum_1^n \dfrac{1}{k!}$ *ne converge pas dans* $\mathbb{Q}$.
- $\mathbb{Q}, \|_p$ *n'est pas complet a titre d'exemple considérons le cas* $p = 5$

  soit la suite $\{\alpha_n\}$ *définit par :*

$$(s) = \begin{cases} \alpha_n^2 + 1 \equiv 0 \ \ (5^n) \\ \alpha_{n+1} \equiv \alpha_n \ \ (5^n) \end{cases}$$

  vérifions qu'une telle suite existe (par récurrence)

  $\alpha_1 = 2 : \alpha_1^2 + 1 = 5 \equiv (5)$,

  $\alpha_2 = 7 : \alpha_2^2 + 1 = 50 \equiv (5^2)$, *et* $\alpha_2 = 7 \equiv \alpha_1 = 2\ (5)$, *supposons* α_n *construit vérifiant* $\alpha_n^2 + 1 \equiv 0\ (5^n)$,

  et posons : $\alpha_{n+1} = \alpha_\alpha + k5^n$, k *à déterminer vérifiant* (s).

  Nous avons déjà $\alpha_{n+1} \equiv \ \alpha_n\ (5^n)$,

  cherchons k *vérifiant* $\alpha_{n+1}^2 + 1 \equiv 0\ (5^{n+1})$,

$$\alpha_{n+1}^2 + 1 = \alpha_n^2 + 1 + 2\alpha_n k5^n + k^2 5^{2n},$$

  par hypothèse de récurrence $\alpha_n^2 + 1 = k_1 5^n$,

nous voulons $\alpha_{n+1}^2 + 1 \equiv 0\ (5^{n+1})$,

soit $5^n(k_1 + 2\alpha_n k) \equiv 0\ (5^{n+1})$, *il suffit pour cela d'avoir* $k_1 + 2\alpha_n k \equiv 0\ (5)$, *comme* $\alpha_n^2 + 1 \equiv 0\ (5^n)$ *alors* $2\alpha_n \equiv 0\ (5)$.

L'application de $\mathbb{Z}/5\mathbb{Z} \longrightarrow \mathbb{Z}/5\mathbb{Z}$ *tel que* $\overline{x} \longmapsto \overline{2\alpha_n x}$ *est bijective, il existe donc* x *tel que* $\overline{2\alpha_n x} = -\overline{k_1}$,

pour $k = x \quad 2\alpha_n k + k_1 \equiv 0\ (5)$.

Si la suite (α_n) *est couverte dans* $\mathbb{Q}$ *sa la suite* α *vérifie* $\alpha^2 + 1 = 0$ *donc* $\alpha \notin \mathbb{Q}$.

2.4 Étude de $\mathbb{Q}_p$

1. Si $|b|_p < |a|_p$ alors $|a + b|_p = |a|_p$.

   Preuve.

   Par (2.4) $|a + b|_p < |a|_p$ ensuite, $a = a + b - b$ donc

   $$|a|_p \leqslant \max\{|a + b|_p, |b|_p\}.$$

   Comme $|a|_p$ n'est pas $\leqslant |b|_p$ alors

   $$|a|_p \leqslant |a + b|_p,$$

   d'où

   $$|a + b|_p = |a|_p = \max\{|a|_p, |b|_p\}.$$

   ■

2. de (1) en déduit

   $$A = \{|a|_p, a \in \mathbb{Q}_p\} = \{|x|_p, x \in \mathbb{Q}\} = B$$

   $$\mathbb{Q} \subset \mathbb{Q}_p \Longrightarrow B \subset A$$

   réciproquement, soit $x \in A\ \exists \alpha \in \mathbb{Q}_p$, $x = |\alpha|_p$. Par la complétion de $\mathbb{Q}$ par $\mathbb{Q}_p$

   $$\exists a \in \mathbb{Q}, \quad |a - \alpha|_p < |\alpha|_p,$$

   donc par (1)

   $$|a|_p = |a - \alpha + \alpha|_p = |\alpha|_p.$$

3. L'ensemble $\{\alpha \in \mathbb{Q}_p \ |\alpha|_p \leqslant 1\}$ est appelé ensemble des entier p-adique, il est noté $\mathbb{Z}_p$ par (2.4) $\mathbb{Z}_p$ est un anneau car

$$|\alpha|_p, |\beta|_p \leqslant 1 \Longrightarrow |\alpha + \beta|_p \leqslant 1; \quad |\alpha\beta|_p \leqslant 1.$$

4. Une nombre rationnel est dans $\mathbb{Z}_p$ si et seulement si il est de la forme $\frac{\upsilon}{\vartheta}$ $\upsilon, \vartheta \in \mathbb{Z}$ $p \nmid \vartheta$

5. Les nombres $\varepsilon \in \mathbb{Q}_p$, tel que $|\varepsilon|_p = 1$ sont les unités p-adiques, ce sont les éléments inversibles dans $\mathbb{Z}_p$

   - Tout élément de $\mathbb{Q}_p^*$ s'écrit $p^n\varepsilon$ avec ε unité, $n \in \mathbb{Z}_p$ Si $\beta \in \mathbb{Q}_p^*$

$$\beta = |\beta|_p \frac{1}{|\beta|_p}\beta = p^n\varepsilon.$$

   - Les unités sont exactement les éléments ε de $\mathbb{Q}_p$ tel que ε et ε^{-1} sont dans $\mathbb{Z}_p$

     Preuve.
     si ε et ε^{-1} sont dans $\mathbb{Z}_p$ alors $|\varepsilon|_p \leqslant 1$, $\frac{1}{|\varepsilon|_p} \leqslant 1$ d'où $|\varepsilon|_p = 1$ et donc ε est une unité, réciproquement, si ε est une unité $|\varepsilon|_p = 1$ et $\varepsilon \in \mathbb{Z}_p$ $|\frac{1}{\varepsilon}|_p = 1$ et $\varepsilon^{-1} \in \mathbb{Z}_p$. ■

6. **Lemme 2.4.1** $\sum \alpha_n$ *convergence* $\Longleftrightarrow \lim \alpha_n = 0$.

   Preuve. $\Longrightarrow$ évident (comme dans $\mathbb{R}$)

   $\Longleftarrow$

$$|\sum_0^N \alpha_n - \sum_0^M \alpha_n|_p = |\sum_{N+1}^M \alpha_n|_p \leqslant \max_{N<n\leqslant M} |\alpha_n|_p,$$

   comme α_n tend vers 0 alors $\Sigma_1^n \alpha_i$ est de Cauchy. ■

7. Description de $\mathbb{Z}_p$

   Soit $A = \{0, 1, ..., p-1\}$

   Les éléments de $\mathbb{Z}_p$ sont exactement les éléments de la forme

$$\sum a_n p^m, \quad a_n \in A \ \ \forall n \in N.$$

Par ce qui précède $\Sigma a_n p^m$ est converge et sa limite est dans $\mathbb{Z}_p$

Réciproquement soit $\alpha \in \mathbb{Z}_p$ donné. Comme $\bar{\mathbb{Q}} = \mathbb{Q}_p$ $\exists\ b\ \in \mathbb{Q}$ tel que $|b - \alpha| < 1$.

2 cas se présente

- Si $|\alpha|_p < 1$ alors $|b| < 1$ $a_0 = 0$ donne $|a_0 - b| < 1$.

- Si $|\alpha|_p = 1$ alors $|b| = 1$ aussi donc $b = \dfrac{\upsilon}{\vartheta}$, $p \nmid \upsilon$, $p \nmid \vartheta$
  $x - \dfrac{\upsilon}{\vartheta} = \dfrac{x\vartheta - \upsilon}{\vartheta}$ l'application de T_ϑ, $\dfrac{\mathbb{Z}}{p\mathbb{Z}} \longrightarrow \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ définit par $\bar{x} \longrightarrow \overline{x\vartheta}$ est surjective car injective donc $\exists\ a_0 \in A$ tel que $a_0\vartheta = \upsilon(\mod p)$ c'est à dire $\exists\ a_0 \in A\ |a_0 - b|_p < 1$
  Maintenant on $|b - \alpha|_p < 1$ et $|a_0 - b|_p < 1$ donc

$$|a_0 - \alpha|_p = |a_0 - b + b - \alpha|_p \leqslant \max |a_0 - b|_p, |b - \alpha|_p < 1$$

  il existe donc $\alpha_1 \in \mathbb{Z}_p$ tel que $| - a_0 + \alpha| = p\alpha_1$ i.e $\alpha = a_0 + p\alpha_1$,
  continuons ainsi avec $\alpha_1 = a_1 + p\alpha_2$ et en continuant ce procédé ou aboutit à

$$\alpha = a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + p^{n+1}\alpha_{n+1},$$

  le résultat s'ensuit.

Chapitre 3

Principe de hasse ou Principe Local-Global

3.1 Lemme de Hensel

Revenons à notre probléme, pour $P \in \mathbb{Q}[X_1, \ldots, X_n]$ homogène, cherchons si $P(X_1, \ldots, X_n) = 0$ possède des solution dans $\mathbb{Q}$ ou ce qui revient ou même des solutions dans $\mathbb{Z}$ car

$$(x_1, \ldots, x_n) \text{ solution} \Longleftrightarrow (\lambda x_1, \ldots, \lambda x_n) \text{ solution}, \ \lambda \in \mathbb{Q}^*.$$

Pour p donné si $P(x_1, \ldots, x_n) = 0$ n'a pas de solution dans $\mathbb{Q}_p$, alors c'est termine il n'y a pas de solution dans $\mathbb{Q}$, passons ou p suivant etc...
Nous voyons qu'il y a des chances que cela ne ce terminé jamais mais heureusement il y le lemme de Hensel.

* D'abord il n'y a qu'un nombre fini de p ou $\overline{F(X)}$ mod p est singulière.

* Si $\overline{F(X)}$ n'est pas singulière, elle possède toujours des solutions mod p.

* Lemme de Hensel : toute solution non singulière de $\overline{F}$ peut être redressé en une solution dans $\mathbb{Q}_p$ de F.

  Ainsi le lemme règle le problème pour presque tout les p, il ne reste qu'un nombre fini de p à traiter.

3.2 Principe de hasse

Considérons toujours l'équation définie sur $\mathbb{Q}, F(x_1, \ldots, x_2) = 0$ et posons nous la question de l'existence de solution rationnelle. Supposons que pour tout p premier l'on puisse montre que F admet une solution dans $\mathbb{Q}_p$ et qu'elle a aussi une solution dans $\mathbb{R}$.

En général c'est facile de voir qu'elle a une solution dans $\mathbb{R}$. Pour presque tous les polynômes $P(x_1, \ldots, x_n) = 0$ possède des solutions non singulières mod p de sorte que l'on puisse appliquer le lemme de Hensel. Il ne restera à traiter qu'un nombre fini de p.

Hasse a été ébloui par les travaux de Minkowski pour la formulation du théorème de Legendre que montre qu'une forme quadratique représente 0 dans $\mathbb{Q}$ si et seulement si elle représente 0 dans $\mathbb{R}$ et dans tous les $\mathbb{Q}_p$ ce qui ressoud le problème d'existence par bloc ou classe de polynômes, et introduit le principe Local-Global ou principe de Hasse.

Étudier un problème sur $\mathbb{Q} \Longleftrightarrow$ Étudier le problème sur les $\mathbb{Q}_p$ et $\mathbb{R}$.

Nous allons montre dans ce qui suit que les formes quadratiques a trois variable vérifie le principe de Hasse. Pour résoudre $q(x_1, \ldots, x_n) = 0$ dans $\mathbb{Q}$, il suffit de résoudre $q(x_1, \ldots, x_n) = 0$ dans $\mathbb{R}$ et dans tous les $\mathbb{Q}_p$.

Malheureusement le Principe de Hasse n'est pas valide pour les cubiques non singulières sinon ou aurait résolu beaucoup de probléme pour les courbes elliptiques. Pour cela nous étudierons le fameux exemple de Selmer.

3.3 Obstruction au principe de Hasse

Commençons pas montrer qu'elle n'a pas de solution dans $\mathbb{Q}$ (non triviales).

Lemme 3.3.1 *soit $a, b, c > 1$ des entiers et supposons $d = abc$ non divisible par un cube et supposons qu'il existe x, y, z non tous nuls tel que $ax^3 + by^3 + cz^3 = 0$ alors il existe $u, v, w \in \mathbb{Z}$ avec $w \neq 0$ tel que $u^3 + v^3 + dw^3 = 0$*

Preuve.

soit $1, \rho, \rho^2$ les racines troisième de l'unité i.e les solutions de $X^3 - 1 = 0$

posons

$$\xi = ax^3 + \rho by^3 + \rho^2 cz^3,$$

et

$$\eta = ax^3 + \rho^2 by^3 + \rho cz^3,$$

donc

$$\xi + \eta = 2ax^3 + (\rho + \rho^2)(by^3 + cz^3) = 3ax^3.$$

De la même manière

$$\rho^2\xi + \rho\eta = 3by^3, \qquad \text{et} \qquad \rho\xi + \rho^2\eta = 3cz^3,$$

maintenant

$$(\xi + \eta)(\rho^2\xi + \rho\eta)(\rho\xi + \rho^2\eta) = \xi^3 + \eta^3 = 3^3(xyz)^3 d,$$

alors $\xi^3 + \eta^3 + d\gamma^3 = 0$ où $\gamma = -3xyz$.

Les deux points $A = (\xi, \rho\eta, \gamma)$ et $B = (\eta, \rho^2\xi, \gamma)$ sont des solutions de l'équation à la courbe $U^3 + V^3 + dW^3 = 0$.

Les points A et B sont conjugués dans $\mathbb{Q}$, donc la droite passant par ces points coupe la courbe en un troisième point défini sur $\mathbb{Q}$ et différent de $(1, -1, 0)$ (puisque ce dernier n'est pas sur la droite). ■

Définition 3.3.2 *(Point exceptionnel) Soit $p = p_0$ un point sur la courbe elliptique (C). La tangente en $P = P_0$ à (C) coupe (C) en un troisième point P_1.*

La tangente en $P = P_1$ à (C) coupe (C) en un troisième point P_2.
De façon générale : la tangente en P_i à (C) coupe (C) en un troisième point P_{i+1}. P est alors dit point exceptionnel si l'ensemble $\{P_0, P_1, \ldots, P_n, \ldots\}$ est fini.

Lemme 3.3.3 *Il n'y a pas de points exceptionnels sur la courbe $X^3 + Y^3 + 60Z^3 = 0$ autre que $(1, -1, 0)$.*

Preuve.

a) $(1, -1, 0)$ est exceptionnel. En effet la tangente à $(1, -1, 0)$
a pour équation $X + Y = 0$ qui coupe $X^3 + Y^3 + 60Z^3 = 0$ en $(1, -1, 0)$.

b) Soit $(x, y, z) \neq (1, -1, 0)$ un point rationnel de $X^3 + Y^3 + 60Z^3 = 0$.
Supposons x, y, z entiers sans facteurs communs ils sont donc premiers deux à deux.
Soit (x_1, y_1, z_1) le troisième point sur $X^3 + Y^3 + 60Z^3 = 0$ et la tangente en (x, y, z) avec (x_1, y_1, z_1) entiers sans facteurs communs.
On peut alors vérifier que :

$$(x_1 : y_1 : z_1) = (x(x^3 + 2y^3) : -y(2x^3 + y^3) : z(x^3 - y^3))$$

Soit d le pgcd de $x(x^3 + 2y^3), -y(2x^3 + y^3), z(x^3 - y^3)$. Si p (p premier) divise x et d alors il divise aussi y contradiction.
Donc d divise $x^3 + 2y^3$ et $2x^3 + y^3$, donc d divise aussi $3x^3$ et $2y^3$ d'où $d = 1$ ou $d = 3$, Ainsi

$$z_1 = \pm z(x^3 - y^3) \qquad \text{ou} \qquad z_1 = \pm z(\frac{x^3 - y^3}{3})$$

Dans tous les cas $|z_1| > |z|$. En répétant ce procédé (de la tangente) ou obtient des points distincts de la courbe $X_1, X_2, \ldots$ vérifiant $|z| < |z_1| < |z_2| < \ldots$

on en déduit que (x, y, z) n'est pas exceptionnel et ne peut donc pas être de torsion.

■

Lemme 3.3.4 *la courbe $x^3 + y^3 + 60z^3 = 0$ est birationnellement équivalente à*

$$Y^2 = X^3 - 2^4 3^2 60^2 = X^3 - 432d^2,$$

avec $d = 60$.

Preuve.

Soit

$$E_1 : x^3 + y^3 = d,$$

et

$$E_2 : Y^2 = X^3 - 432d^2,$$

le changement de variable rationnel

$$x = \frac{36d + Y}{6X} \qquad \text{et} \qquad y = \frac{36d - Y}{6X}$$

admet un changement inverse unique

$$X = \frac{12d}{x + y} \qquad \text{et} \qquad Y = \frac{36d(x - y)}{x + y}$$

et les équations E_1 et E_2 sont birationnellement équivalentes. ■

Lemme 3.3.5 *$X^3 + Y^3 + 60z^3$ est birationnellement équivalente $Y^2 = X^3 - 432(60)^2$ birationnellement équivalente à $Y^2 = X^3 - 3^3 30^2$ pour lequel $A/2A$ est trivial.*

Preuve.

Par les lemmes la courbe $3X^3 + 4Y^3 + 5Z^3$ n'a pas de points non triviaux définis sur $\mathbb{Q}$.
En effet supposons que $3X^3 + 4Y^3 + 5Z^3$ possède une solution non triviale définie sur $\mathbb{Q}$.
Par le lemme 3.3.1 $X^3 + Y^3 + 60Z^3$ possède une solution non triviale (x, y, z).
Par le lemme 3.3.3 $X^3 + Y^3 + 60Z^3$ n'a pas de points exceptionnelles autre que $(1, -1, 0)$ donc (x, y, z) n'est pas exceptionnellement par le lemme 3.3.4 la courbe est birationnelle équivalente à $Y^2 = X^3 - 432.60^2$ et donc aussi à $Y^2 = X^3 - 3^3.30^2$ pour lequel $A/2A$ est trivial.

$\rightarrow$ contradiction $\leftarrow$ ■

Pour montrer que la courbe $3X^3 + 4Y^3 + 5Z^3 = 0$ possède des solution dans $\mathbb{Q}_p$ pour tout p nous admettons les résultats suivants :

Théorème 3.3.6 *soit $Y^2 = X^3 + AX + B$ une courbe elliptique définie sur $\mathbb{F}_p$, alors le nombre de points N de $Y^2 = X^3 + AX + B$ définis sur $\mathbb{F}_p$ vérifie*

$$|N - (q + 1)| \leq 2\sqrt{p}.$$

Théorème 3.3.7 *soit D une courbe elliptique définie sur $\mathbb{F}_P$ alors Elle possède un point défini sur $\mathbb{F}_P$.*

Maintenant,la courbe $3X^3 + 4Y^3 + 5Z^3 = 0$ est birationnellement équivalente à $Y^2 = X^3 - 432.60^2$.

La courbe réduite mod p est singulière pour $p = 2, 3, 5$, elle reste non singulière pour tous les $p \neq 2, 3, 5$, est possède par le théorème 3.3.6 un point défini sur $\mathbb{F}_p$.

Théorème 3.3.8 *Si la courbe réduite $\bar{C}$ mod p reste de genre 1 alors le point de la courbe défini sur $\mathbb{F}_p$ peut être redressé en un point de C défini sur $\mathbb{Q}_p$.*

Lemme 3.3.9 *soit $D : F(X_1, X_2, X_3)$ une courbe elliptique définie sur $\mathbb{Q}$ telle que sa réduction modulo p*

$\bar{C} : \bar{F}(X_1, X_2, X_3)$ soit une courbe elliptique sur $\mathbb{Z}/p\mathbb{Z}$

Soit $a \in \mathbb{Z}^3$ tel que $\bar{F}(\bar{a}) = 0$, il existe alors $b \in \mathbb{Z}^3$ tel que

1. $f(b) = 0 \quad (p^2)$.
2. $b \equiv a \quad (p)$.

Plus généralement il existe une suite (a_k), $a_1 = a$, $a_2 = b$

1. $f(a_k) \equiv 0 \quad (p^k)$.
2. $a_k \equiv a_{k-1} \quad (p^{k-1})$.

Preuve.

Pour $k = 2$ c'est la première partie du lemme nous avons $\frac{\partial f}{\partial X_i}(\bar{a}) \equiv 0$ pour un $i \in \{1, 2, 3\}$ par exemple $\frac{\partial f}{\partial X_i}(\bar{a}) \equiv 0$ ($\bar{C}$ non singulière)

posons $b = (b_1, b_2, b_3) = a + \alpha p = (\alpha_1 + \alpha_1 p, a_2 + \alpha_2 p, a_3 + \alpha_3 p)$

(2) est alors vérifie $b \equiv a \quad (p)$

cherchons α pour que (1) le soit aussi.

Le développement de Taylor de F au voisinage de a donne :

$$F(X_1, X_2, X_3) = F(a) + \sum \Big(\frac{\partial f}{\partial X_i}\Big)_a (X_i - a_i) + \text{terme de degré} \geq 2.$$

$$F(b_1,b_2,b_3)=F(a)+\sum\Big(\frac{\partial f}{\partial X_i}\Big)_a(\alpha_i p)+\text{terme multiple de } p^2.$$

Prenons $\alpha_2=\alpha_3=0, F(a)=kp$ (car$\equiv 0(p)$), en obtient

$$F(b)=kp+\rho_1\alpha_1 p=p(k+\rho_1\alpha_1),\qquad (\frac{\partial f}{\partial X_1}(a)=\rho_1)$$

choisissons α_1 tels que $(k+\rho_1\alpha_1)=0$, et c'est possible car $\rho_1\neq 0\ (p)$ et donc ρ_1 inversible dans $\mathbb{Z}/p\mathbb{Z}$

$\alpha_1=-\rho_1^{-1}k$, ainsi $F(b)\equiv 0 \quad (p^2)$

supposons $a_1\dots a_k$ construit et construisons a_{k+1}

en posant $a_{k+1}=a_k+\alpha p^k$, (2) est alors vérifiée

$$F(\alpha_{k+1})=F(\alpha_k)+\sum(\frac{\partial f}{\partial X_i})_{\alpha_k}\alpha_i p^k+\text{termes}\equiv 0\ p^{2k},$$

$$Kp^k+\rho_1\alpha_1 p^k \quad \text{on prend} \quad \alpha_1=-\rho_1^{-1}K.$$

La suite (α_k) est une suite de Cauchy qui converge donc vers un élément x_0 de $\mathbb{Q}_p$ et $F(\alpha_k)$ est aussi une suite de Cauchy qui converge vers 0, comme F est continue

$$0=\lim F(\alpha_k)=F(\lim\alpha_k)=F(x_0).$$

Pour les p rendant la courbe réduite singulière c'est à $p=2,3$ ou 5, nous résolvons directement l'équation $3x^3+4y^3+5z^3=0$,

$p=5$ on prend $z=0$, $x=1$, et nous cherchons $y\in\mathbb{Q}_5$ tels que $3+4y^3=0$ ou $y^3=-\dfrac{3}{4}=-\dfrac{6}{8}$,

comme -8 est un cube, il suffit de prouver que 6 est un cube i.e $y^3=6$ possédé des solution dans $\mathbb{Q}_p$.

$$\alpha_k^3-6\equiv 0\ 5^k,$$

soit $\alpha_1,\alpha_2,\dots,\alpha_k$

$$\alpha_k^3-6\equiv 0\ 5^k,$$

$$\alpha_{k+1}\equiv\alpha_k\ (5^k),$$

α_1 donc $1^3-6=-5\equiv 0\ (5^1)$.

Supposons α_k construit et soit $\alpha_{k+1} = \alpha_k + \rho 5^k$, ρ à déterminer

$$\alpha_{k+1}^3 - 6 = \alpha_k^3 - 6 + 3\alpha_k^2 \rho 5^k + 3\alpha_k \rho^2 5^{2k} + \rho^3 5^{3k}$$

$$\equiv \rho_1 5^K + 3\alpha_k^2 \rho 5^k \ (5^{k+1}),$$

comme $3\alpha_k^2$ étant unité ou prend $\rho = \dfrac{-1}{3\alpha_k^2}\rho_1$.

De la même manière

pour $p = 3$ $\quad x = 0, z = -1$ et l'on calcule y solution de $4y^3 - 5 = 0$ dans $\mathbb{Q}_3$.

pour $p = 2$ $\quad y = 0, z = 1$ et l'on calcule x solution de $3y^3 + 5 = 0$ dans $\mathbb{Q}_2$.

■

CONCLUSION

Soit $F(X, Y, Z)$ un polynôme homogène de $\mathbb{Q}[X, Y, Z]$.

$$F(X, Y, Z) = 0 \text{ résoluble dans } \mathbb{Q} \Rightarrow F(X, Y, Z) = 0 \text{ résoluble dans } \mathbb{R} \text{ et dans tous les } \mathbb{Q}_p$$

l'implication inverse n'est malheureusement vraie que pour certaines classes d'équations.
Une classe d'équations $\mathfrak{S}$ vérifie le principe de Hasse si et seulement si $\forall F \in \mathfrak{S}$

$$F(X, Y, Z) = 0 \text{ dans } \mathbb{Q} \text{ résoluble} \Longleftrightarrow F(X, Y, Z) = 0 \text{ résoluble dans } \mathbb{R} \text{ et dans tous les } \mathbb{Q}_p$$

Enfin nous étudions une d'équation de dégre 3 à savoir $3X^3+4Y^3+5Z^3 = 0$ qui ne vérifie pas le principe de hasse.

Bibliographie

[1] Arnélie Schinck , *The Local-Global Principle in Number Theory.*Presented in Partial Fulfillment of the Requuements for the Degree of Master of Science at Concordia University Montréal, Québec, Canada.OAméiie Schinck, 2001.

[2] D.Harary, Principe local-global en arithmétique.

[3] Francis Nier Dargoç Iftimie , *Introduction à la Topologie.* université de Rennes 1.

[4] J.Cassels, Arithmitique des courbes elliptiques.

[5] KEITH CONRAD, *The Local-Global Principale.*

[6] KEITH CONRAD, *Selmer's exemple.*

[7] Z.I.BOREVITCH et I.R.CHAFAREVITCH, *Théorie des nombres.*Traduit par Myriam et Jean-Luc VERLEY.GAUTHIER-VILLARS PARIS, 1967.

[8] Yichang CAI et Nicolas MOUTAL, *Le théorème de Hasse-Minkowski.*sous la supervision de Diego IZQUIERDO.