UNIVERSITE KASDI MERBAH OUARGLA
Faculté des Mathématiques et des Sciences de la Matière

N° d'ordre :
N° de série :

DEPARTEMENT DE MATHEMATIQUES

MASTER

Spécialité : Mathématiques

Option : Algébre et Géométrie

Par : Baghdadi Bouthaina

Thème

Théoréme de Legendre

Soutenu publiquement le : 25/05/2017

Devant le jury composé de :

Benmoussa M.Tayeb	Prof. Université KASDI Merbah- Ouargla	Président
M.Amine Bahayou	M.A. Universié KASDI Merbah- Ouargla	Examinateur
Yasssine Guerboussa	M.A. Université KASDI Merbah- Ouargla	Examinateur
Boussaid Mouhamed	M.A. Universié KASDI Merbah- Ouargla	Examinateur
M.LAid Youmbai	M.C. Université KASDI Merbah- Ouargla	Rapporteur

Dédicaces

Nous avons commencé plus d'une main plupart d'entre eux et nous avons beaucoup souffert de difficultés et maintenant nous sommes aujourd'hui et heureusement implique des nuits blanches et des jours pénibles et récapitulation Emczuarna entre les couvertures de ce modeste travail.

Dans un phare de la science et de l'imam Mustafa à un analphabète qui a enseigné Altalim au maître de la création de notre noble Prophète Muhammad paix soit sur lui.

Pour la fontaine, qui ne se lasse pas de donner à mon bonheur imité tissé avec des fils de son coeur à ma chère mère.

Pour le méchant et cherché à alléger le plus doux et le contentement qu'il a donné quelque chose à la charge dans la voie du succès qui a élevé lui m'a appris que la vie avec sagesse et patience à mon père.

Consacrer tous mes remerciements et le respect à mon cher marie HAMZA et son appréciation pour ma situation de se tenir avec moi et pour chaque tout famille BAFFI .

Pour leur amour d'être dans mes veines et mon coeur médite leur mémoire à mes frères et soeurs.

De marchaient ensemble pour et nous faisons notre chemin ensemble vers le succès et la créativité de la main dans la main et nous en prenons la fleur et appris à mes amis et collègues.

Remerciement

Avant toute considération,je remercie le Grand Dieu le tout puissant qui, m'a aidé pour achever ce travail.

Je tiens tout a remercier premier lieu mon encadreur Monsieur "M.L AID YOUMBAI" de m'avoir proposé un des plus importants thèmes et pour sa continuité à me soutenir et à m'encourager. Je voudrai aussi le remercier pour sa gentillesse, sa disponibilité et du temps consacré à mon travail.

Je remercie également les membres du département de Mathématique et Informatique de m'avoir permis de travailler dans de bonnes conditions pendant la réalisation de mon travail.
Merci également a tous les enseignants qui m'ont aidé pendant mon cursus (GUERBOUSSA , BENMOUSSA ,BAHAYOU) sans oublier leurs conseils précieux.

Je remercie aussi toute personne de prés ou de loin a contribué à la finalisation de ce travail.

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.

➤ $(x_n)_{n\in\mathbb{N}}$: suite de Cauchy.

➤$\widehat{x}$: la classe d'équivalence.

➤$\|$: valeur absolue sur K.

➤ $\|_\infty$: valeur absolue archimédienne.

➤ $\|_p$: valeur absolue p-adique.

➤ $d_{\|}$: la distance induite sur K.

➤ $\mathbb{Z}_p$: l'ensemble des entier p-adique.

➤ $\mathfrak{C}$: l'ensemble des suite de Cauchy dans $\mathbb{Q}, \|_p$.

➤ $\mathfrak{N}$: les sous ensemble de $\mathfrak{S}$.

➤ $\mathfrak{M}$: idéal de $\mathfrak{S}$.

➤ Λ : sous groupe de $\mathbb{Z}^n$.

INTRODUCTION

Soit $P(x, y, z) \in \mathbb{Z}[x, y, y]$ homogène.
Si $P(x, y, z) = 0$ possédé des solutions non toutes nulle dans $\mathbb{Z}$ alors elle possédé 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 de est regarder si elle n'a pas de solution $\mod p$; si elle en a de a des solutions mod p on étudier à l'équation $\mod p^2$, $\mod p^3$, $\mod p^4, \ldots$.
C'est pour traiter tous ces cas d'un seul coup que Hansel 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

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

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

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

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

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 plus pratiquement $\mathbb{Q}_p$ et $\mathbb{Z}_p$.

Dans ce chapitre 1, nous présentons la complétion d'un espace métrique en général comme vu en cours de topologie 2^{eme} année.

Nous exposons dans ce chapitre 2 les valeurs absolues sur un corps en général et insistons sur la valeur absolue non archimédienne sur le corps des rationnels $\mathbb{Q}$. Nous complétions alors $\mathbb{Q}, \|_p$ pour obtenir $\mathbb{Q}_p$(Nous nous familiarisons enfin avec les nombre p-adiques).

Dans ce chapitre 3 présente sa validité pour les formes quadratiques à trois variable.

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 1.1.1

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

l'espace métrique (X, d) est **complet** si toute suite de Cauchy converge.

Exemple 1.3.1

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* $\mathbb{R}$ *(puisque* $[-M, M]$ *est compact). Mais alors la Proposition(1.2.2) 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 1.3.1 *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 $x, y, z \in C_X$

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

   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 $k\geq\max\{k_n,k_m\}$

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

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 :

$$\delta(x[x_n], x) = \lim_{k\to\infty} d(x_n, x_k) \leq \varepsilon$$

pour tout $\varepsilon > 0$ 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 (2.1) et (2.2) montre que $|1| = 1(x = y = 1), |1| = 1(x = y = 1)$ puisque $|\frac{1}{x}| = \frac{1}{|x|}$.

Définition 2.1.2

(Valeur absolue trivial)

La valeur absolue triviale est définie par :

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

- ***(valeur absolue archimédienne sur $\mathbb{Q}$)***

  L'application de $\mathbb{Q}$ dans $\mathbb{R}_+$ définie par :

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

  est une valeur absolue sur $\mathbb{Q}$.

- ***(valeur absolue p-adique sur $\mathbb{Q}$)***

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

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

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

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 nous donne :

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

et démontre l'égalité (2.2).

D'autre part, en supposant que $k \leqslant k'$ (sinon 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 $ad+cbp^{k'-k} = p^r a'$ avec $(a',p) = 1$ 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 $\mathbb{R}$ induite 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 :*

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

Exemple 2.1.1 *Nous savons que la valeur absolue triviale*

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

induit la distence triviale

$$(x,y) \longrightarrow d(x,y) = \begin{cases} 0 & si \quad x = y \\ 1 & sinon \end{cases}$$

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

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

Définition 2.1.5

- *On appelle corps valué , 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 défnie par*

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

- *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 2.1.6 *Soit k un corps et $\|\|_1, \|\|_2$ deux valeurs absolues sur k.*
Les valeurs absolues $\|\|_1$ et $\|\|_2$ sont équivalentes ssi pour toute suite $(x_n)_{n\in\mathbb{N}}$ de k $(|x_n|_1 \underset{n\longrightarrow+\infty}{\longrightarrow} 0) \Leftrightarrow (|x_n|_2 \underset{n\longrightarrow+\infty}{\longrightarrow} 0)$.

Preuve.

$\Longrightarrow$ Supposons que les valeurs absolues $\|\|_1$ et $\|\|_2$ sont équivalentes.
Soit $(x_n)_n \geqslant 0$ une suite de k convergeant vers 0 pour la distance d_1. Alors, pour tout ouvert V de 0 (pour la distance d_2), il existe un rang n_0 tel que $\forall n \geqslant n_0$, $u_n \in V$ .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 $(|x_n|_1 \underset{n\longrightarrow+\infty}{\longrightarrow} 0 \Leftrightarrow (|x_n|_2 \underset{n\longrightarrow+\infty}{\longrightarrow} 0)$.
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 ssi pour toute suite $(x_n)_n \geqslant 0$ d'éléments de F convergeante 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 convergeante vers $x \in F$ 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 fermè 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 2.1.7 *Soint $\|\|_1$ et $\|\|_2$ deux valeurs absolus sur k, alors $\|\|_1$ et $\|\|_2$, sont équivalente ssi il existe un réel positif a tel que :*

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

Preuve.

L'implication réciproque est évidente grace au lemme.

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 $|x|_2^n = |x^n|_2 \underset{n\longrightarrow+\infty}{\longrightarrow} 0$ 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 $\dfrac{p}{q} < b$, on a les équivalences suivantes :

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

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 remplacant 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 :

$$|\frac{x}{x_0}|_1 = |\frac{x}{x_0}|_2^a \Longleftrightarrow |x|_1 = |x|_2^a$$

(car $|x_0|_1 = |x_0|_2^a$) , ce qui nous permet d'affirmer :

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

■

Corollaire 2.1.8 *Deux valeurs absolues $\|_p$ et $\|_1$ sont équivalentes ssi $p = l$.*

Preuve.

La réciproque est triviale.

Pour l'implication directe, il suffit de considérer la suite (p^n) $n > 0$. 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 2.1.9 ***(Ostrowski)*** *Toute valeur absolue sur $\mathbb{Q}$ est équivalente à l'une des valeurs absolues suivantes :*

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

Preuve.

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

- 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 $(|n^k| = |n|^k)_k$ 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 $|n'| < 1$ (si non 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'hypothése). Pour ce nombre n' , il existe des nombres premiers $p_1, .., p_r$ deux à deux distincts et des entiers positifs $l_1, .., l_r$ tels que $n' = \pm p_1^{l_1}...p_r^{l_r}$ donc $|p_1|^{l_1}...|p_r|^{l_r} = |n'| < 1$.
  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 théoréme 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 :

$$|a_k p^k| = |a_k|\ |p|^k \leqslant_{(5)} |p^k| \xrightarrow[k\longrightarrow+\infty]{} 0 \text{ et } |b_k n^k| = |b_k||n| \leqslant_{(5)} |n|^k \xrightarrow[k\longrightarrow+\infty]{} 0$$

  On en déduit que :

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

  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 $x = p^k \frac{a}{b}$ avec $(a, p) = (b, p) = 1$ donc :

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

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

- Cas où $\mathbb{Z}$ 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 :

  $$n = \Sigma_{m=0}^{r_n} q_m a^m$$

  avec $k_m \in \{0, ..., a-1\}, q_{r_n} \neq 0$ et $r_n \leqslant \dfrac{lnn}{lna}$ (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 :

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

  D'autre part, pour tout entier k, l'entier n^k peut s'écrire $n^k = \sum_{m=0}^{r_n} q'_m a^m$ avec $r_n k \leqslant \dfrac{lnn^k}{lna}$ ce qui nous fournit l'inégalité :

  $$\forall k \in \mathbb{N}, \quad |n|^k = |n^k| \leqslant \sum_{k=0}^{r_n k} |a|^k.$$

  Supposons qu'il existe un entier $a > 1$ tel que $|a| \leqslant 1$. Alors l'inégalité (2.1) 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 :

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

  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 borné pour $\|$ ce qui est absurde.

  Ainsi pour tout entier naturel $a > 1$, on a $|a| > 1$. Nous reprenons l'inégalité (2.1) pour un entier $a > 1$ (donc $|a| > 1$ ce qui nous donne :

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

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

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

$$-\frac{1}{k}\ln(|a|^{k\frac{lnn}{\ln a}+1}) \underset{k\longrightarrow+\infty}{\sim} k\frac{\ln n}{\ln a}\ln|a| \underset{k\longrightarrow+\infty}{\longrightarrow} \frac{\ln n}{\ln a} ln|a| \ .$$

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

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

Si l'on échange le rôle de a et de$n$ dans l'inéquation précédente, on obtient que le rapport $\frac{ln|a|}{lna}$ est constant sur les entiers strictements 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 ($d = \frac{\overbrace{\ln|a|}^{>0}}{\underbrace{\ln a}_{>0}}$ pour tout entier $a>1$) et plus petit que 1 ($|a| = \underbrace{|1+1+1+...|}_{afois} \leqslant |a|_\infty |1| = a$)
Ainsi, si $\mathbb{Z}$ est un ensemble borné pour $\|$, alors $\|$ est équivalente à la valeur absolue archimédienne $\|_\infty$.

■

Définition 2.1.10 *Une valeur absolue sur $\mathbb{Q}$ est dite :*

- *Archimédienne ssi elle est équivalente à la valeur absolue $\|_\infty$.*
- *Non archimédienne ssi elle est équivalente à une certaine valeur absolue p-adique.*

2.2 Complétion

Définition 2.2.1 *Une corps K est dite complet par rapport à la valeur absolue $\|$ ssi toute suite de Cauchy dans K est converge.*

Définition 2.2.2 *On dit que la corps $K, \|\|\|$ est le complété du 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 $\mathbb{Q}$

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

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

Soit $\mathfrak{N}$ le sous ensemble de $\mathfrak{C}$ formé des suites qui tendent vers 0.
$\mathfrak{N}$ est un idéal maximal de $\mathfrak{C}$ de sorte que $\dfrac{\mathfrak{C}}{\mathfrak{N}}$ soit un corps, il sera note $\mathbb{Q}_p$. Définition de la valeur absolue sur $\mathfrak{C}$

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

sinon :

$$\{a_n\} \in \mathfrak{C}_1, \{a_n\} \notin \mathfrak{N}.$$

alors :

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

donc :

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

Posons $|\{a_n\}|_p = |a_N|_p$.

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

Soit $\mathfrak{M} \supset \mathfrak{N}$ un idéal de $\mathfrak{C}, \mathfrak{M}$ contient un élément $\{a_n\} \notin \mathfrak{N}, \{a_n\} \in \mathfrak{C}$, 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 $\{a_n^{-1}\} \in \mathfrak{C}$ et $\{a_n^{-1}\}\{a_n\} \in \mathfrak{M} \Longrightarrow \mathfrak{M} = \mathfrak{C}$, d'où $\mathfrak{N}$ maximal et $\dfrac{\mathfrak{C}}{\mathfrak{N}}$ corps.

Soit l'application :

$$\begin{aligned} \mathbb{Q} &\xrightarrow{\lambda} \frac{\mathfrak{C}}{\mathfrak{N}} \\ a &\longrightarrow \overline{\{a\}} \end{aligned}$$

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

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

Exemple 2.3.1

- $\mathbb{Q}$ *muni de la valeur absolus triviale est complet .*
- $\mathbb{Q}, \|_\infty$ *n'est pas complet . La suite*

$$x_n = \sum_0^n \frac{1}{k!}$$

ne converge pas dans $\mathbb{Q}$*.*

- $\mathbb{Q}, \|_p$ *n'est pas complet à titre d'exemple le cas* $P = 5$

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

$$(S) = \begin{cases} \alpha_n^2 + 1 \equiv & 0 \ (5^n) \\ \alpha_n + 1 \equiv & \alpha_n \ (5^n) \end{cases} \tag{2.6}$$

Vérifions qu'une telle suite existe (par récurence)

$\alpha_1 = 2 : \alpha_1^2 + 1 = 5 \equiv 0 \ (5)$

$\alpha_2 = 7 : \alpha_2^2 + 1 = 50 \equiv 0 \ (5^2)$ *et* $\alpha_2 = 7 \equiv \alpha_1 = 2 \ (5)$

Supposons α_n construit vérifiant $\alpha_n^2 + 1 \equiv 0\ (5^n)$ et posons :

$\alpha_{n+1} = \alpha_n + k5^n$ *, k à détérminer vérifiant (S) .*

Nous avons déja $\alpha_{n+1} \equiv \alpha_n\ (5^n)$ cherchons k verifiant :

$\alpha_{n+1}^2 + 1 \equiv 0\ (5^{n+1})$ $\alpha_{n+1}^2 + 1 = \alpha_n^2 + 1 + 2\alpha_n k5^n + k^2 5^{2n}$.

Par hypothése 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 $2\alpha_n \ncong 0\ (5)$.

L'application de $\dfrac{Z}{5Z} \longrightarrow \dfrac{Z}{5Z}$ telle que $\bar{x} \longmapsto \overline{2\alpha_n x}$ est bijective , il existe donc x telle que $\overline{2\alpha_n x} = \overline{-k_1}$,

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

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

2.4 Etude de $\mathbb{Q}_p$

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

Preuve.

Par (2.3) $|a + b|_p < |a|_p$ 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 $|a + b|_p = |a|_p = Max\{|a|_p, |b|_p\}$.

- de (2.1) 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 $\mathbb{Q}_p$

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

donc par (2.1) $|a|_p = |a - \alpha + \alpha|_p = |\alpha|_p$.

- L'ensemble $\alpha \in \mathbb{Q}_p \quad |\alpha|_p \leqslant 1$ est appelé ensemble des entier p-adique , il est note $\mathbb{Z}_p$ par ((2.3)) $\mathbb{Z}_p$ est un anneau car $|\alpha|_p, |\beta|_p \leqslant 1 \Longrightarrow |\alpha + \beta|_p \leqslant 1$,
  $|\alpha\beta|_p \leqslant 1$. (2.4)

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

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

  1. Tout élément de $\mathbb{Q}_p^*$ s'écrit $p^n\varepsilon$ avec ε unité $n \in \mathbb{Z}_p$
     Si $\beta \in \mathbb{Q}_p^*$ $\beta = |\beta|_p \ \frac{1}{|\beta|_p}\beta = p^n\varepsilon$.

  2. Les unités sont exactement les éléments ε de $\mathbb{Q}_p$ tel que 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 $\varepsilon \in \mathbb{Z}_p$ $|\varepsilon|_p = 1$ et $\varepsilon^{-1} \in \mathbb{Z}_p$.

■

- **Lemme 2.4.1** $\sum \alpha_n$ *converge* $\Longleftrightarrow \lim \alpha_n = 0$.

  Preuve.

  $\Longrightarrow$: evident (comme dans $\mathbb{R}$) .

  $\Longleftarrow$: $|\sum_0^N \alpha_n - \sum_0^M|_p = |\sum_{N+1}^M \alpha_n|_p \leqslant \max_{N<n\leqslant M} |\alpha_n|_p$ comme α_n tend vers 0 alors $\Sigma_1^n \alpha_i$ est de Cauchy .

- Déscription de $\mathbb{Z}_p$

  Soit $A = 0, 1, ..., p-1$.

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

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

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

  Réciproquement soit $\alpha \in \mathbb{Z}_p$ donné comme $\bar{\mathbb{Q}} = \mathbb{Q}_p$. $\quad \exists\, b \in \mathbb{Q}$ tel que $|b - \alpha| < 1$ 2 cas se presente :

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

– Si $|\alpha|_p = 1$ alors $|b| = 1$ aussi donc $b = \dfrac{\upsilon}{\vartheta}$ $\quad p \nmid \upsilon$ $p \nmid \vartheta$

$x - \dfrac{\upsilon}{\vartheta} = \dfrac{x\vartheta - \upsilon}{\vartheta}$

L'application de T_ϑ $\quad \dfrac{\mathbb{Z}}{\mathbb{P}\mathbb{Z}} \longrightarrow \dfrac{\mathbb{Z}}{\mathbb{P}\mathbb{Z}}$ définit par $\bar{x} \longrightarrow \bar{x\vartheta}$ est surjective car injective donc $\exists$ $a_0 \in A$ tel que $a_0\vartheta = \upsilon \pmod p$ 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 $| - a_0 + \alpha| = p\alpha_1$ ie $\alpha = a_0 + p\alpha_1$ continuons ainsi avec $\alpha_1 = a_1 + p\alpha_2$ en continiant ce précédé on aboutit à

$\alpha = a_0 + a_1 p + a_2 p^2 + ... + a_n p^n + p^{n+1}\alpha_{n+1}$ le résultat s'ensuit .

■

Chapitre 3

Théoréme de Legendre

3.1 Réseaux de $\mathbb{R}^n$

Soit $\mathbb{R}^n$ l'éspace vectoriel des n-upplets $x = (x_1, x_2, ..., x_n)$. Il contient le groupe $\mathbb{Z}^n$ des x pour les quels $x_i \in \mathbb{Z}$.

Soit $S \subset \mathbb{R}^n$, on note $v(S)$ où $\varsigma(S)$ le volume de S qui est simplement sa mesure de le besgues

Lemme 3.1.1 ***(Blichfeldt)***

Soit $m > 0$ un entier naturel et $S \subset \mathbb{R}^n$ avec $v(S) > m$, il existe alors $m + 1$ éléments de $S : s_0, s_1, ..., s_m$ tels que :

$$s_i - s_j \in \mathbb{Z}^n \quad 0 \leqslant i, j \leqslant m.$$

Preuve.

Soit $W \subset \mathbb{R}^n$ le cube unité des points

$$w = (w_1, w_2, ..., w_n) \ \setminus \ 0 \leqslant w_j < 1 \ , \ 1 \leqslant j \leqslant n \ .$$

Tout $x \in \mathbb{R}^n$ s'écrit de manière unique :

$$x = w + z \quad z \in \mathbb{Z}^n \quad w \in W \ .$$

Soit ψ la fonction caracteristique de S $m < v(S) = \int\limits_{\mathbb{R}^n} \psi(x)dx \qquad (\mathbb{R}^n = \bigcup\limits_{w\in W} \bigcup\limits_{z\in\mathbb{Z}^n} \{w+z\}$

$$= \int\limits_W (\sum_{z\in\mathbb{Z}^n} \psi(w+z))dw$$

Comme $v(w) = 1$ alors il existe $w_0 \in w \backslash \sum \psi(w_0+z) > m$, où encore $\sum\limits_{z\in\mathbb{Z}^n} \psi(w_0+z) \geqslant m+1$
Considérons alors $s_j = w_0 + z$ pour les quels $\psi(w_0 + z) > 0$

$$s_j - s_k = (w_0 + z_j) - (w_0 + z_k) = z_j - z_k \in \mathbb{Z}^n \ .$$

■

Définition 3.1.2 *L'ensemble S est dit symétrique (par rapport à 0) si :*

$$x \in S \Longrightarrow -x \in S$$

il est dit convexe si :

$$x, y \in S \Longrightarrow \lambda x + (1-\lambda)y \in S \quad 0 \leqslant \lambda \leqslant 1$$

En particulier $(\lambda = \frac{1}{2})$ le milieu $\frac{1}{2}(x+y)$ de $[x \ \ y]$ est dans S .

Théorème 3.1.3 ***(Minkowski** $m = 1$**)*** *Soit Λ un sous groupe de $\mathbb{Z}^n$ d'indice n .*
Soit $C \subset \mathbb{R}^n$ un ensemble symétrique convexe de volume $V(C) > 2^n m$.
Alors C et Λ ont un point commun autre que $O = (0, 0, ..., 0)$.

Preuve.
Soit $S = \frac{1}{2}C = \{\frac{1}{2}c \ \ , c \in C\}$ alors :

$$V(\frac{1}{2}C) = \frac{1}{2^n}V(C) > m \ .$$

Par le lemme précédent , il existe $m+1$ élément $c_0, c_1 ... c_m$ telle que
$\frac{1}{2}c_i - \frac{1}{2}c_j \in \mathbb{Z}^n \ \ 0 \leqslant i, j \leqslant m$. Le $m+1$ élément $\frac{1}{2}c_0 - \frac{1}{2}c_i \quad 0 \leqslant i \leqslant m$ sont à répertir partir dans m classes d'élément de $\mathbb{Z}^n$ modulo $\Lambda \quad (z_1 + \Lambda, z_2 + \Lambda, ..., z_m + \Lambda)$, il y a donc deux élément qui sont necéssairment dans la même classe

$$\frac{1}{2}c_0 - \frac{1}{2}c_i \text{ et } \frac{1}{2}c_0 - \frac{1}{2}c_j \quad 0 \leqslant i, j \leqslant m \quad i \neq j$$

sont de la même classe $z_k + \Lambda$. D'où $(\frac{1}{2}c_0 - \frac{1}{2}c_j) - (\frac{1}{2}c_0 - \frac{1}{2}c_i) \in \Lambda$

$$\alpha = \frac{1}{2}c_i - \frac{1}{2}c_j \in \Lambda$$

Comme C est symétrique alors $-c_j \in C$ et comme elle est aussi convexe
$\frac{1}{2}c_i + (\frac{1}{2}(-c_j)) \in C$ donc $\alpha \in \Lambda \cap C$, il est n'est pas égale à 0 car $c_i \neq c_j$. ■

Lemme 3.1.4 *Soit N un entier positif et supposons : $\exists\ l \in \mathbb{Z} : l^2 \equiv -1$ (mod N) alors $N = u^2 + v^2$ pour $u, v \in \mathbb{Z}$.*

Preuve.

Soit $n = 2$

Prenons pour C le disque $0 < x^2 + y^2 < 2N$ de volume (suface) 2^2N

Soit Λ le sous groupe de $\mathbb{Z}^2$ donné par : $(x, y) \in \mathbb{Z} \quad y = lx \pmod{n}$, il est clairement d'indice N ■

3.2 Principe de Hassse pour les coniques

Définition 3.2.1 *Une conique C définie sur $\mathbb{Q}$ est donnée par une équation de la forme :*

$$C : F(X) = \sum f_{ij} X_i X_j$$

où $X = (X_1, X_2, X_3)$; $f_{ij} = f_{ji} \in \mathbb{Q}$

Lorsque $F(X)$ est le produit de deux polynomes de 1^{er} degré, elle est singuliére et ne considérons pas ce cas.

Les coniques restantes sont non singuliéres et $\det f_{ij} \neq 0$.

Un critére pour l'existence de point rationnel sur une conique est donné par legendre ; Hasse a donné sa formulation .

Théorème 3.2.2 *Une condition necessaire et suffisante par l'existence d'un point rationnel sur C est qu'il existe un point de C définit sur $\mathbb{R}$ et un point de C défini sur $\mathbb{Q}_p$ pour*

tout p , puisque la condition est évident trivialement nécessaire .

Nous allons dans ce qui suit nous préparer pour la démonstration de la suffisance .

3.2.1 Transformation sur une conique :

Une transformation :

$$T : X_i = \sum_j t_{ij} Y_j \ .$$

Avec $t_{ij} \in \mathbb{Q}$ transforme la forme quadratique $F(X)$ en la forme quadratique $G(Y)$.

Tout point défini sur $\mathbb{Q}$ sur $F(X) = 0$ est transformé en un point définit sur $\mathbb{Q}$ sur $G(Y)$.

La transformation inverse T^{-1} fait correspondre les points de $G(Y) = 0$ aux points sur $F(X) = 0$.

Nous avons les mémes résultats pour les points définis sur $\mathbb{Q}_p$ et ceux définie sur $\mathbb{R}$.

Ainssi la principe de Hasse est vérifié pour $F(X) = 0$ si et s'il verifié pour $G(Y) = 0$.

Maintenant un bon choix de la transformation T nous permet de ne considère que les coniques de la forme :

$$F(X) = f_1 X_1^2 + f_2 X_2^2 + f_3 X_3^2$$

Le changement de variable $X_j \longrightarrow t_j X_j \quad t_j \in \mathbb{Q}$, nous permet de supposer sans restriendre la généralité que : $f_j \in \mathbb{Z}$ $j = 1, 2, 3$ et f_j sans facteur carré .

Si f_1, f_2, f_3 ont p comme facteur commun , nous remplaçons $F(X)$ par $\dfrac{1}{p} F(X)$.

Si deux des f_j (f_1, f_2par exemple) sont divisibles par p et $p \nmid f_3$, nous remplacons X_3 par pX_3 puis nous divisons $F(X)$ par p .

Ainssi , pour prouver le Théoreme , il suffit de le prouver pour les coniques de la forme :

$$F(X) = f_1 X_1^2 + f_2 X_2^2 + f_3 X_3^2 = 0$$

avec $f_j \in \mathbb{Z}$ et $f_1 f_2 f_3$ sans facteur carré .

Ensuite nous supposons que $F(X) = 0$ posséde des points localement (définis sur $\mathbb{Q}_p$ et $\mathbb{R}$) .

$C : F(X) = 0$ posséde un point défini sur $\mathbb{Q}_p$, s'il existe

$a = (a_1, a_2, a_3) \neq (0, 0, 0)$ tel que $F(a) = 0$ $a_j \in \mathbb{Q}_p$ bien entendu.

Sans restreindre la généralité , on peut supposer (on multiplira si nécessaire les a_j par un élément de $\mathbb{Q}_p$) que $\max |a_j|_p = 1$

Considére alors les cas suivants :

- première cas : $p \neq 2 \quad p/f_1 f_2 f_3$ et sans restreindre la généralité p/f_1 $p \nmid f_2$ $p \nmid f_3$ donc $|f_1 a_1^2|_p < 1$, supposons aussi si possible $|a_2|_p < 1$ d'où :

  $$|f_3 a_3^2|_p = |f_1 a_1^2 + f_2 a_2^2|_p < 1 \text{ et donc } |a_3|_p < 1 \ .$$

  Maintenant :

  $$|f_1 a_1^2|_p = |f_2 a_2^2 + f_3 a_3^2|_p \leqslant p^{-2}$$

  et donc $|a_1|_p < 1$ puisque f_1 sans facteur carré .

  Ceci contredit le fait que $\max\{|a_j|_p\} = 1$ (3.2.1) , donc $|a_2|_p = |a_3|_p = 1$

  mais comme $|f_2 a_2^2 + f_3 a_3^2|_p < 1$ et en divisant par l'unite a_2 , on déduit l'existence d'un $r_p \in \mathbb{Z}$ tel que :

  $$f_2 + r_p^2 f_3 \equiv 0(p).$$

- Deuxiéme cas : $p = 2$ $2 \nmid f_1 f_2 f_3$ a) Deux des a_j sont des unités .

  En effet $\max |a_j|_p = 1 \Longrightarrow$ il y a une unité des ons $|a_2|_p = 1$

  $$|f_1 a_1^2|_p = |f_2 a_2^2 + f_3 a_3^2|_p \leqslant \max\{|f_2 a_2^2|_p, |f_3 a_3^2|_p\} \leqslant \max\{1, |f_3 a_3^2|_p\}$$

  Si $|a_3^2|_p \neq 1$ alors $|f_1 a_1^2|_p = \max\{1, |f_3 a_3^2|_p\} = 1$ et $|a_1^2|_p = 1$ c'est à dire a_1 ou a_3 est unité .

  Supposons $|a_2|_p = 1$ et $|a_3|_p = 1$.

  Nous avons :

  $$\overline{f_2 a_2^2 + f_3 a_3^2} = \overline{f_1 + f_2} = 0(2)$$

  d'où :

  $$\overline{f a_1^2} = \overline{a_1^2} = 0(2)$$

  mais la classe d'un carré est égale 0 (4) d'où $f_1 + f_2 \equiv 0$ (4) .

- Troixiéme cas : $p = 2$ $2/f_1f_2f_3$ ($2/f_1$ $2 \nmid f_2$ $2 \nmid f_3$ par exemple)

  commençons par montrer que $|a_2|_2 = |a_3|_2 = 1$

  $\max_j\{|a_j|_2\} = 1$ deux cas possible à priori

  1. $|a_2|_2 = 1$ où $|a_3|_2 = 1$ disons $|a_2|_2 = 1$ $|f_1a_1^2|_2 = |f_2a_2^2+f_3a_3^2|_2 \leqslant \max\{|f_2a_2^2|_2, |f_3a_3^2|_2\}$
     $\leqslant \max\{1, |f_3a_3^2|_2\}$ comme $|f_1a_1^2| < 1$ alors $|f_3a_3^2|_2 = |a_3^2|_2 = 1$

  2. $|a_2|_1 < 1$ et $|a_2|_1 < 1$ donc $|a_1|_2 = 1$ car $\max\{|a_1|_2, |a_2|_2, |a_3|_2\} = 1$

     Paraillons :

     $$\overline{a_2^2} \equiv 0\ (4) \text{ et } \overline{a_3^2} \equiv 0(4)$$

     d'où :

     $$\overline{f_1a_1^2} = \overline{f_1} = \overline{f_2a_2^2 + f_3a_3^2}$$
     $$\equiv 0\ (4)\ f_1 \equiv 0\ (4) \text{ contredit le fait que } 2^2 \nmid f_1\ .$$

     Maintenant :

     $$|a_2|_2 = |a_3|_2 = .1$$

     - Si $|a_1|_2 < 1$ alors $\overline{f_1a_1^2} = 0\ (8)$ donc aussi $\overline{f_2a_2^2 + f_3a_3^2} = 0\ (8)$ et
       $f_2 + f_3 \equiv 0\ (8)$.
     - Si $|a_1|_2 = 1$ en plus de $|a_2|_2 = |a_3|_2 = 1$

       $f_1a_1^2+f_2a_2^2+f_3a_3^2 = 0 \Longrightarrow \overline{f_1a_1^2 + f_2a_2^2 + f_3a_3^2} = 0(8) \Longrightarrow f_1+f_2+f_3 = 0(8)$

       car :

       $$\overline{a_1^2} \equiv \overline{a_1^2} \equiv \overline{a_1^2} \equiv 1(8).$$

     En resumé

     Les coniques considérés ont été reduites à la forme :

     $$f_1X_1^2 + f_2X_2^2 + f_3X_3^2 = 0$$

     où :

     $$f_1, f_2, f_3 \in \mathbb{Z}\ \ ;\ \ f_1f_2f_3$$

sans facteurs carrés .

Nous avons supposé que la conique possède des points localement et on obtenu les résultats suivants :

(a) Si $p \neq 2$ $p/f_1f_2f_3$ p/f_1 , alors $\exists r_p \in \mathbb{Z}$ tel que $f_2 + r_pf_3 \equiv 0\ (p)$.

(b) Si $p = 2 \nmid f_1f_2f_3$ alors sans restreindre la généralité
$f_2 + f_3 \equiv 0\ (4)$.

(c) Si $p = 2\ / f_1f_2f_3$ alors $s^2f_1f_2f_3 \equiv 0\ (8)$ $s = 0$ où 1 .
Nous imposons alors aux réseau Λ les congurence dans le 1^{er} cas : $x_3 = r_px_2^2$ pour obtenir
$F(x) = f_1x_1^2 + f_2x_2^2 + f_3r_p^2x_3^2$
$\equiv (f_2 + r_p^2f_3)x_2^2\ mod\ p$
$\equiv 0\ (p)$
nous imposons dans le 2^{nd} cas :

$$x_1 \equiv 0\ (2)$$
$$x_1 \equiv x_3\ (2)$$

ce qui implique :

$$F(x) \equiv 0\ (4)$$

Dans le 3^{eme} cas imposerons :

$$x_1 \equiv x_3\ (4)$$
$$x_1 \equiv x_3\ (4)$$

on obtient :

$$F(x) \equiv 0\ (8)$$

En fin avec un réseau Λ d'indice $m = 4|f_1f_2f_3|$ dans $\mathbb{Z}^3$ on obtient :

$$F(x) \equiv 0\ (4|f_1f_2f_3|) \text{ pour } \underset{(x_1,x_2,x_3)}{x} \in \Lambda$$

Soit $C \in \mathbb{R}^n$ l'ellipsoide symétrique convexe :

$$f_1X_1^2 + f_2X_2^2 + f_3X_3^2 < 4|f_1f_2f_3|$$

dont le volume est $V(C) = \dfrac{4}{3}\ \Pi\ 2^3|f_1f_2f_3| > 2^3m$, il existe donc $x \neq 0$ $c \in C \cap \Lambda$ pour cet x on a :

i. $F(x) \equiv 0\ (4|f_1 f_2 f_3|)$.

ii. $|F(x)| \leqslant |f_1|X_1^2 + |f_2|X_2^2 + |f_3|X_3^2 < 4|f_1 f_2 f_3|$

d'où

$$F(x) = 0$$

Conclusion

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

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

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

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

Enfin nous étudions la classe d'équation des formes quadratiques à trois variabele qui verifie le principe de Hasse.

Bibliographie

[1] D.Harry,Principe loca-qlobal enarthmétique .

[2] J.Cassels ,Aritmetique des courbes elliptiques .

Introduction à la Topologie. université de Rennes 1.

[3] Legendre transforms Mark Alford, Jan 2015 Francis Nier Dargoç Iftimie ,

[4] LEGENDRE'S THEOREM, LEGRANGE'S DESCENT SUPPLEMENT FOR MATH 370 : NUMBER THEORY.

[5] LES NOMBRES p-ADIQUES, NOTES DU COURS DE M2 par Pierre Colmez

[6] Yichang CAI et Nicolas MOUTAL,Le théoréme de Hasse-Minkowski.sous la supervision de Diego IZQIERDO .

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