Théorèmes d'Ostrowski et de Hasse-Minkowski

Titouan Olivier-Choupin

Stage de magistère à l'Institut Fourier
Encadré par Tanguy Rivoal
Juin 2025

Table des matières

1 Corps valués

1.1 Valeurs absolues

On cherche ici à généraliser le rôle que l'application module joue sur $\mathbb{C}$ (et donc par restriction que la valeur absolue usuelle joue sur $\mathbb{R}$ ou $\mathbb{Q}$). Ceci permettra notamment par la suite d'étendre la notion d'espace vectoriel normé à des corps de base plus généraux que $\mathbb{R}$ ou $\mathbb{C}$ (non nécessairement de caractéristique 0, par exemple).

La notion de valeur absolue est la notion centrale de cette section. La définition qui suit est la plus communément adoptée (voir par exemple [1, p.118]).

Définition 1.1 (Valeur absolue)**.** *On appelle valeur absolue sur un corps K toute application $|\cdot| : K \to \mathbb{R}_+$ vérifiant les axiomes suivants :*

(i) $\forall x \in K, |x| = 0 \Leftrightarrow x = 0$ *(séparation) ;*

(ii) $\forall x, y \in K, |xy| = |x||y|$ *(multiplicativité) ;*

(iii) $\forall x, y \in K, |x + y| \leq |x| + |y|$ *(inégalité triangulaire).*

En pratique, on utilisera la définition suivante tirée de [4, p.63] dont on s'inspirera beaucoup dans cette première sous-section. Cette définition moins restrictive (sans toutefois avoir un champ d'application plus général comme on le verra par la suite) a pour intérêt principal de simplifier quelques raisonnements.

Définition 1.2 (Valeur absolue étendue)**.** *On appellera valeur absolue étendue sur un corps K (abrégé v.a.e.), une application $|\cdot|$ de K dans $\mathbb{R}_+$ vérifiant les axiomes de séparation et de multiplicativité ainsi que la propriété suivante :*

(iii′) $\exists C \in \mathbb{R}_+, \forall x, y \in K, |x + y| \leq C \max(|x|, |y|)$ *(inégalité triangulaire étendue).*

De plus l'infimum des C vérifiant (iii′) sera qualifié de constante de la valeur absolue étendue $|\cdot|$.

Définition 1.3 (Corps valué (étendu))**.** *Un corps valué est la donnée $(K, |\cdot|)$ d'un corps K et d'une valeur absolue $|\cdot|$ sur K. On dira parfois par abus de langage que K est un corps valué en supposant implicitement qu'il est muni d'une valeur absolue. On parlera également de corps valué étendu pour qualifier un corps muni d'une v.a.e..*

Toute valeur absolue est une *v.a.e.* ce qui permet notamment de parler de la constante d'une valeur absolue. L'inégalité triangulaire donne que la constante d'une valeur absolue est inférieure ou égale à 2. La réciproque est en fait vraie.

Proposition 1.4. *Une v.a.e. sur un corps K est une valeur absolue si et seulement si sa constante est inférieure ou égale à 2.*

Démonstration. Soit $|\cdot|$ une *v.a.e* de constante C. S'il s'agit d'une valeur absolue, alors pour $x, y \in K$, on a $|x+y| \leq |x| + |y| \leq 2\max(|x|, |y|)$. En particulier, $C \leq 2$.

Réciproquement, si $C \leq 2$, montrons que $|\cdot|$ vérifie l'inégalité triangulaire. Pour commencer, soit $n \in \mathbb{N}$. On a $|n| \leq 2n$. En effet, on encadre n entre 2^r et 2^{r+1} pour un certain entier r. On écrit alors n comme une somme de 2^{r+1} terme valant 0 ou 1. En appliquant $n+1$ fois l'inégalité triangulaire étendue, on obtient $|n| \leq C^{r+1}\max(|0|, |1|) \leq 2^{r+1} \leq 2n$.

Soient maintenant $x, y \in K$. En appliquant n fois de façon dichotomique l'inégalité triangulaire étendue à la somme de 2^n termes

$$(x+y)^{2^n-1} = \sum_{i=0}^{2^n-1} \binom{2^n-1}{i} x^i y^{2^n-1-i},$$

on obtient :

$$\begin{aligned}
|x+y|^{2^n-1} &\leq C^n \max\left\{ \left| \binom{2^n-1}{i} \right| |x|^i |y|^{2^n-1-i}, 0 \leq i \leq 2^n-1 \right\} \\
&\leq 2^n \times 2\max\left\{ \binom{2^n-1}{i} |x|^i |y|^{2^n-1-i}, 0 \leq i \leq 2^n-1 \right\} \\
&\leq 2^{n+1} \sum_{i=0}^{2^n-1} \binom{2^n-1}{i} |x|^i |y|^{2^n-1-i} = 2^{n+1}(|x|+|y|)^{2^n-1}.
\end{aligned}$$

Ainsi, $|x+y|^{2^n-1} \leq 2^{n+1}(|x|+|y|)^{2^n-1}$. En passant au logarithme, en divisant par 2^n-1 et en prenant la limite quand n tend vers l'infini, on obtient $|x+y| \leq |x| + |y|$. □

Puisque pour toute *v.a.e*, on a $|1| = 1$ et $|-1| = 1$, la constante d'une *v.a.e.* est toujours supérieure ou égale à 1. Ceci justifie la définition suivante.

Définition 1.5. *Une v.a.e. $|\cdot|$ sur un corps K sera dite non archimédienne (ou ultramétrique) si sa constante vaut 1 et archimédienne si elle est strictement supérieure à 1.*

Notons en particulier qu'une *v.a.e.* non archimédienne est une valeur absolue. Donnons quelques exemples de valeurs absolues pour illustrer les notions introduites jusqu'à maintenant.

- Sur tout corps K, on définit une valeur absolue dite triviale en posant $|0| = 0$ et $\forall x \in K^\times, |x| = 1$. Cette valeur absolue est non-archimédienne.

- La valeur absolue usuelle sur $\mathbb{C}$ (ou sur $\mathbb{R}$ ou $\mathbb{Q}$) est archimédienne de constante 2.
- Soit K un corps, on pose pour tous polynômes $P, Q \in K[X]$ avec $Q \neq 0$ $\deg\left(\frac{P}{Q}\right) = \deg(P) - \deg(Q)$. Alors, pour tout $\gamma > 1$, on obtient une valeur absolue sur $K(X)$ en posant $|R|_\infty = \gamma^{\deg(R)}$. C'est une valeur absolue ultramétrique.
- Si $|\cdot|$ est une *v.a.e.* sur un corps K alors $|\cdot|^t$ est également une *v.a.e.*.

Le dernier exemple justifie la définition suivante.

Définition 1.6 (Valeurs absolues équivalentes)**.** *Deux valeurs absolues (étendues)* $|\cdot|_1$ *et* $|\cdot|_2$ *sur un corps* K *sont dites équivalentes s'il existe* $t > 0$ *tel que* $|\cdot|_1^t = |\cdot|_2$.

Notons que le fait d'être équivalent est une relation d'équivalence. On verra plus tard qu'une *v.a.e.* ne nous intéresse en fait qu'à équivalence près. On constate de plus que si $|\cdot|_1$ et $|\cdot|_2 = |\cdot|_1^t$ sont deux *v.a.e.* équivalentes de constantes respectives C_1 et C_2 alors $C_2 = C_1^t$. On en déduit en particulier les faits suivants.

- Toute *v.a.e.* est équivalente à une valeur absolue (en utilisant la proposition 1.4).
- Deux *v.a.e.* équivalentes sont simultanément archimédiennes ou ultramétriques.

Voici maintenant une notion qui permet de donner de nouveaux exemples de valeurs absolues ultramétriques.

Définition 1.7 (Valuation)**.** *On appelle valuation sur un* K *une application* $v : K^\times \to \mathbb{R} \cup \{+\infty\}$ *vérifiant les axiomes suivants :*

(i) $\forall x \in K, v(x) = +\infty \Leftrightarrow x = 0$;

(ii) $\forall x, y \in K, v(xy) = v(x) + v(y)$;

(iii) $\forall x, y \in K, v(x+y) \geq \min(v(x), v(y))$.

De plus, si $v(K^\times)$ *est un sous-groupe discret de* $\mathbb{R}$*, on parle de valuation discrète.*

Étant donné $c \in]0,1[$, on dispose d'une bijection entre les valuations et les valeurs absolues ultramétriques d'un corps K. En effet, si v une valuation, c^v est une valeur absolue ultramétrique et réciproquement, si $|\cdot|$ est une valeur absolue ultramétrique, $\log_c(|\cdot|)$ est une valuation. Ceci montre que l'étude des valeurs absolues ultramétriques se ramène à celle des valuations. On utilisera ces deux notions tout au long de cet article.

- Soit A un anneau factoriel et $p \in A$ irréductible. On définit ce qu'on appelle la valuation p-adique sur A par $v_p(a) = \max\{n \in \mathbb{N}, p^n | a\}$. On étend cette fonction au corps de fraction K de A en posant $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$ et c'est alors une valuation au sens de la définition précédente. Étant donné $c \in]0,1[$, on définit donc une valeur absolue ultramétrique $|\cdot|_p$ sur K en posant pour tout $x \in K$, $|x|_p = c^{v_p(x)}$. Cette valeur absolue est ultramétrique.

- En particulier, en considérant un nombre premier $p \in \mathbb{N}$ et en prenant $c = \frac{1}{p}$, l'exemple ci-dessus définit une valeur absolue ultramétrique sur $\mathbb{Q}$ qu'on appelle valeur absolue p-adique.
- La valeur absolue $|\cdot|_\infty$ précédemment définie sur $K(X)$ par $|P|_\infty = \gamma^{\deg(P)}$ est un cas particulier de notre premier exemple en prenant $A = K[\frac{1}{X}]$, $p = \frac{1}{X}$ et $c = \frac{1}{\gamma}$.

On donne maintenant une caractérisation particulièrement utile pour identifier si une *v.a.e.* est ou non archimédienne. Pour cela, on commence par noter $i(\mathbb{Z})$ l'image de $\mathbb{Z}$ par l'unique morphisme d'anneau i de $\mathbb{Z}$ dans K. Pour $n \in \mathbb{Z}$, on se permettra d'écrire n au lieu de $i(n)$.

Proposition 1.8. *Une v.a.e. $|\cdot|$ sur un corps K est ultramétrique si et seulement si elle est bornée sur $i(\mathbb{Z})$. De plus, on a alors $\forall n \in \mathbb{Z}, |n| \leq 1$.*

Démonstration. Si $|\cdot|$ est ultramétrique, alors

$$\forall n \in \mathbb{N}, |n| = |1 + 1 + \cdots + 1| \leq \max(|1|, |1|, \ldots, |1|) = 1.$$

De plus, $|-n| = |-1||n| \leq 1$. En particulier, $|\cdot|$ est bornée sur $i(\mathbb{Z})$.
Réciproquement, supposons $|\cdot|$ bornée sur $i(\mathbb{Z})$. Soit $|\cdot|_2$ une valeur absolue équivalente à $|\cdot|$. On va montrer que $|\cdot|_2$ est ultramétrique ce qui impliquera que $|\cdot|$ l'est. Soit $x, y \in K$ avec $|x| \geq |y|$. Pour tout $n \in \mathbb{N}$, on a alors

$$|(x+y)^n| = \left|\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}\right| \leq \sum_{i=0}^{n} \left|\binom{n}{i}\right| |x|^i |y|^{n-i} \leq \sum_{i=0}^{n} |x|^i |y|^{n-i} \leq (n+1)|x|^n.$$

En prenant la racine n-ième, on a donc $|x+y| \leq (n+1)^{\frac{1}{n}}|x|$ et donc en passant à la limite quand n tend vers l'infini, on obtient $|x+y| \leq |x| = \max(|x|, |y|)$, ce qu'on voulait. □

Cette caractérisation permet en particulier de constater que le caractère archimédien d'un corps valué étendu est invariant par extension. Si en effet, $(K, |\cdot|_K)$ et $(L, |\cdot|_L)$ sont des corps valués étendus avec $K \subset L$ et si la restriction de $|\cdot|_L$ à K est $|\cdot|_K$ (on dit que $|\cdot|_L$ prolonge $|\cdot|_K$) alors $|\cdot|_K$ est ultramétrique si et seulement si $|\cdot|_L$ l'est.

Cette constatation va notamment nous permettre de remarquer qu'une valeur absolue sur un corps de caractéristique non nulle est ultramétrique. Commençons par une proposition caractérisant les valeurs absolues sur les corps finis.

Proposition 1.9. *Une v.a.e. sur un corps fini est nécéssairement triviale.*

Démonstration. Soit K un corps fini de cardinal q et $|\cdot|$ une valeur absolue sur K. Soit $x \in K^\times$. On a $x^{q-1} = 1$. Ainsi $|x|^{q-1} = 1$ et comme $x \in \mathbb{R}_+$, on a $|x| = 1$, ce qui montre que $|\cdot|$ est triviale. □

Corollaire 1.10. *Une v.a.e. sur un corps de caractéristique non nulle est ultramétrique.*

Démonstration. En effet, soit un corps K de caractéristique p munit d'une valeur absolue $|\cdot|$. Comme K contient $\mathbb{F}_p$, et la restriction de $|\cdot|$ à $\mathbb{F}_p$ est triviale, donc ultramétrique, $|\cdot|$ est ultramétrique. □

1.2 Topologie d'un corps valué

1.2.1 Topologie et équivalence de valeurs absolues

De tels corps sont naturellement munis d'une structure d'espace topologique. On verra de plus que d'un point de vue topologique, la notion de corps valué étendu n'est pas plus large et qu'on peut donc toujours se ramener à celle de corps valué.

Définition 1.11 (Boule ouverte)**.** *Soit $(K, |\cdot|)$ un corps valué. Soient $x \in K$ et $r > 0$. On appelle :*

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

La notion de boule ouverte permet alors de définir une topologie sur K :

Définition 1.12. *Soit $(K, |\cdot|)$ un corps valué. La topologie induite par $|\cdot|$ sur K est la topologie engendrée par les boules ouvertes.*

Donnons quelques exemples de topologies sur des corps valués.

- Sur $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$, la topologie induite par la valeur absolue usuelle coïncide avec la topologie usuelle sur ces ensembles.
- Soit K un corps. La topologie induite sur K par la valeur absolue triviale est la topologie discrète.
- Soit p un nombre premier. La topologie induite sur $\mathbb{Q}$ par la valeur absolue p-adique est qualifiée de topologie p-adique.

Si $|\cdot|$ est une valeur absolue sur K, la topologie induite par $|\cdot|$ est une topologie métrique. En effet, c'est celle qui est donnée par la distance définie sur K par $\forall x, y \in K, d(x,y) = |x-y|$. Si $|\cdot|$ est seulement une *v.a.e.*, d (définie ci-dessus) n'est généralement pas une distance. Toutefois, K est bien un espace métrique : il suffit de constater que sa topologie coïncide avec celle définit sur K par une valeur absolue équivalente à $|\cdot|$. C'est une conséquence immédiate du sens direct de la proposition suivante.

Proposition 1.13. *Soient K un corps et $|\cdot|_1$, $|\cdot|_2$ deux v.a.e. sur K. $|\cdot|_1$, $|\cdot|_2$ sont équivalentes si et seulement si elles induisent la même topologie sur K.*

Pour démontrer cette proposition, on aura besoin du lemme suivant.

Lemme 1.14. *Soit K un corps et $|\cdot|_1, |\cdot|_2$ deux v.a.e. sur K. Si $|\cdot|_1$ est non triviale et si $\forall x \in K, |x|_1 > 1 \Rightarrow |x|_2 > 1$, alors $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes.*

Démonstration. Soit $x \in K^\times$. Si $|x|_1 > 1$, par hypothèse, $|x|_2 > 1$. Si $|x|_1 < 1$ alors $|1/x|_1 > 1$ et donc $|1/x|_2 > 1$ puis $|x|_2 < 1$. Finalement, si $|x|_1 = 1$, comme $|\cdot|_1$ est non triviale, il existe $a \in K^\times$ tel que $|a|_1 < 1$, pour tout entier n, on a alors $|x^n a|_1 < 1$, d'où $|x^n a|_2 < 1$ puis $|x|_2 < |a|_2^{-1/n}$ et donc en faisant tendre n vers l'infini, $|x|_2 \leq 1$. En

appliquant le même raisonnement à $1/x$, on obtient $|x|_2 \geq 1$ et donc $|x|_2 = 1$. On vient de montrer que pour tout $x \in K$, la position par rapport à 1 de $|x|_1$ est la même que celle de $|x|_2$.

Soient maintenant $x, y \in K^\times$. Pour tout $(m,n) \in \mathbb{Z}^2$, les positions par rapport à 1 de $|\frac{x^n}{y^m}|_1$ et $|\frac{x^n}{y^m}|_2$ sont les mêmes. Ainsi, $n\ln(|x|_1) - m\ln(|y|_1)$ et $n\ln(|x|_2) - m\ln(|y|_2)$ sont simultanément positifs, négatifs ou nuls. Dans le cas où $|y|_1 \neq 1$ (et donc $|y|_2 \neq 1$), les majorants et minorants rationels de $\ln(|x|_1)/\ln(|y|_1)$ et $\ln(|x|_2)/\ln(|y|_2)$ sont donc les mêmes, d'où, $\ln(|x|_1)/\ln(|y|_1) = \ln(|x|_2)/\ln(|y|_2)$ puis pour tous $x, y \in K^\times$ avec $|x|_1, |y|_1 \neq 1$, on a $\ln(|x|_1)/\ln(|x|_2) = \ln(|y|_1)/\ln(|y|_1)$. En notant t ce rapport, on a donc $\forall x \in K, |x|_1 = |x|_2^t$, puis $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes. □

Démonstration de la proposition 1.13. Si $|\cdot|_1 = |\cdot|_2^t$ avec $t > 0$, alors pour tout $x \in K$, $B_1(x, r^t) = B_2(x, r)$, ce qui montre $(K, |\cdot|_1)$ et $(K, |\cdot|_2)$ ont les mêmes boules et donc la même topologie.

Réciproquement, supposons que $|\cdot|_1$ et $|\cdot|_2$ induisent la même topologie sur K. Soit $x \in K^\times$ tel que $|x|_1 > 1$. Comme $1/|x|_1^n \xrightarrow[n\to+\infty]{} 0$, la suite $(x_1^{-n})_{n\in\mathbb{N}}$ tend vers 0 dans $(K, |\cdot|_1)$, donc dans $(K, |\cdot|_2)$. Ainsi, $1/|x|_2^n \xrightarrow[n\to+\infty]{} 0$ et donc $|x|_2 > 1$. Le lemme 1.14 permet alors de conclure. □

Comme deux *v.a.e.* équivalentes définissent la même topologie et qu'une *v.a.e.* est toujours équivalente à une valeur absolue, on peut dès maintenant se restreindre à l'étude des valeurs absolues.

Finissons ce paragraphe par un théorème d'approximations simultanées. Celui-ci permet de constater que la non équivalence d'une famille de valeurs absolues correspond à une certaine forme d'indépendance entre elles.

Proposition 1.15. *Soient K un corps et $|\cdot|_1, \ldots, |\cdot|_n$ des valeurs absolues non triviales non équivalentes. Soient $x_1, \ldots, x_n \in K$ et $\varepsilon > 0$. Il existe $x \in K$ tel que $\forall i \in [\![1, n]\!], |x - x_i|_i < \varepsilon$.*

Démonstration. On commence par montrer par récurrence sur $n \geq 2$ qu'il existe $y \in K$ tel que $|y|_1 < 1$ et $\forall i \in [\![2, n]\!], |y|_i < 1$. Comme $|\cdot|_1$ et $|\cdot|_2$ sont non équivalentes et non triviales, le lemme 1.14 montre qu'il existe $a, b \in K$ avec $|a|_1 < 1$, $|a|_2 \geq 1$ et $|b|_2 < 1$, $|b|_1 \geq 1$. Ainsi, $y := \frac{b}{a}$ convient.

Supposons maintenant le résultat au rang $n-1$ et montrons le au rang n. Soit z tel que $|z|_1 < 1$ et $\forall i \in [\![2, n-1]\!], |z|_i < 1$. Si $|z|_n < 1$, $y := z$ convient. Sinon, grâce au cas $n = 2$, on prend $w \in K$ tel que $|w|_1 < 1$ et $|w|_n > 1$. On a $|z^p|_1 \xrightarrow[p\to+\infty]{} +\infty$ et $\forall i \in [\![2, n-1]\!], |z^p|_i \xrightarrow[p\to+\infty]{} 0$. De plus, si $|z|_n > 1$, $|z^p|_n \xrightarrow[p\to+\infty]{} +\infty$, ainsi, $y := \frac{w}{1+z^{-p}}$ convient pour p assez grand. Finalement, si $|z|_n = 1$, $\forall p \in \mathbb{N}, |z^p|_n = 1$ et donc $y := z^p w$ convient pour p assez grand, ce qui achève la récurrence.

Par symétrie, on peut donc prendre $z_1, \ldots, z_n$ tel que $\forall i \in [\![1, n]\!], |z_i|_i > 1$ et $\forall i, j \in [\![1, n]\!], i \neq j \Rightarrow |z_i|_j < 1$. Alors pour tout $i \in [\![1, n]\!]$, $(\frac{1}{1+u_i^{-p}})_{p\in\mathbb{N}}$ tend vers 0 pour $|\cdot|_j$ si

$j \neq i$ et vers 1 pour $|\cdot|_i$. Ainsi, $x := \sum_{i=1}^{n} x_i \frac{1}{1+u_i^{-p}}$ convient pour p assez grand. □

1.2.2 Complétion d'un corps valué

Au même titre qu'on construit $\mathbb{R}$ comme le complété de $\mathbb{Q}$ vis à vis de sa topologie usuelle, on va chercher ici à construire pour un corps valué $(K, |\cdot|)$ un nouveau corps valué qui soit sont complété en tant qu'espace topologique. Plus précisément, on dispose du théorème suivant.

Théorème 1.16. *Soit $(K, |\cdot|_K)$ un corps valué. Il existe un corps valué $(\widehat{K}, |\cdot|_{\widehat{K}})$ tel que :*

- *$\widehat{K}$ contient K et $|\cdot|_{\widehat{K}}$ prolonge $|\cdot|_K$;*
- *$\widehat{K}$ est complet ;*
- *K est dense dans $\widehat{K}$.*

De plus, un tel corps est unique à isomorphisme de corps valué près (un isomorphisme de corps valué étant un isomorphisme de corps et une isométrie (pour les distances induites par les valeurs absolues sur ces corps)).

Démonstration. Montrons d'abord l'existence. On adapte ici la même preuve de la construction de $\mathbb{R}$ par les suites de Cauchy. Considérons l'anneau C_K des suites de Cauchy sur K. L'ensemble I_K des suites tendant vers 0 est un idéal maximal de K si bien que $\widehat{K} := C_K/I_K$ est un corps. Soit π la projection canonique de C_K C_K/I_K. Soit $x := (x_n)_{n\in\mathbb{N}}$ une suite de Cauchy de K alors $(|x_n|_K)_{n\in\mathbb{N}}$ est une suite de Cauchy dans $\mathbb{R}$, donc elle converge vers un réel positif qu'on notera $|x|_{C_K}$. On constate que si $x, y \in C_K$ avec $\pi(x) = \pi(y)$ alors $|x|_{C_K} = |y|_{C_K}$. Ainsi, l'application $|\cdot|_{C_K}$ passe au quotient par I_K fournissant une application $|\cdot|_{\widehat{K}} : \widehat{K} \to \mathbb{R}_+$. On vérifie alors que $|\cdot|_{\widehat{K}}$ est une norme sur $\widehat{K}$.

On a une inclusion naturelle i de K dans $\widehat{K}$ qui à $x \in K$ associe l'image dans C_K/I_K de la suite constante égale à x. La définition de $|\cdot|_{\widehat{K}}$ entraîne alors qu'elle prolonge $|\cdot|_K$.

Montrons maintenant la densité de K dans $\widehat{K}$. Soit $x \in \widehat{K}$. On prend $(x_n)_{n\in\mathbb{N}} \in C_K$ tel que $\pi((x_n)_{n\in\mathbb{N}}) = x$. Soit $\varepsilon > 0$. Comme $(x_n)_{n\in\mathbb{N}} \in C_K$ est de Cauchy, il existe $n \in N$ tel que $\forall p, q \geq N, |x_p - x_q|_K < \varepsilon$. Soit $p > N$, ceci entraîne par définition que $|\pi((x_q - x_p)_{q\in\mathbb{N}})|_{\widehat{K}} < \varepsilon$. Ainsi, $|\pi((x_q)_{q\in\mathbb{N}}) - \pi((x_p)_{q\in\mathbb{N}})|_{\widehat{K}} < \varepsilon$, c'est-à-dire $|x - i(x_p)|_{\widehat{K}} < \varepsilon$ d'où la densité de K dans $\widehat{K}$. On a même montré mieux, à savoir que $(i(x_n))_{n\in\mathbb{N}}$ tend vers $\pi((x_n)_{n\in\mathbb{N}})$ (ce qui est plutôt heureux, car on a construit $\pi((x_n)_{n\in\mathbb{N}})$ pour cela).

Soit $(x_n)_{n\in\mathbb{N}} \in \widehat{K}^{\mathbb{N}}$ de Cauchy. Pour chaque x_n. Par densité de K dans $\widehat{K}$, pour tout $n \in \mathbb{N}$, il existe $y_n \in K$ tel que $|x_n - i(y_n)|_{\widehat{K}} < 1/n$. Le fait que (x_n) soit de Cauchy dans $\widehat{K}$ entraîne alors que (y_n) est de Cauchy dans K. Soit $y = \pi((y_n))$. On a vu précédement que $(i(y_n))_{n\in\mathbb{N}}$ tend vers y. Comme de plus $|x_n - i(y_n)|_{\widehat{K}} < 1/n$, on en déduit que $(x_n)_{n\in\mathbb{N}}$ tend vers x et donc que $\widehat{K}$ est complet.

Montrons maintenant l'unicité. Soit $(K_1, |\cdot|_{K_1})$, $(K_2, |\cdot|_{K_2})$ deux corps valués contenant K et vérifiant les propriétés du théorème. Soit $x \in K$. Par densité de K dans K_1, il existe $(x_n)_{n\in\mathbb{N}} \in K^{\mathbb{N}}$ tendant vers x dans K_1. $(x_n)_{n\in\mathbb{N}}$ est alors de Cauchy, donc converge dans K_2. De plus, si $(y_n)_{n\in\mathbb{N}} \in K^{\mathbb{N}}$ est une autre suite convergent vers x dans K_1, la limite de $(y_n)_{n\in\mathbb{N}}$ dans K_2 est la même que celle de $(x_n)_{n\in\mathbb{N}}$ (car $(x_n - y_n)_{n\in\mathbb{N}}$ tend vers 0 dans K). Ainsi, on dispose d'une application $\phi : K_1 \to K_2$ associant à un élément de $x \in K_1$ la limite dans K_2 de n'importe quelle suite de K tendant vers x dans K_1. On définit de la même façon une application $\psi : K_2 \to K_1$. Il découle alors de leurs définitions que ϕ et ψ sont réciproque l'une de l'autre. Le fait qu'il s'agisse d'isométries et de morphismes de corps vient alors simplement du passage à la limite des différentes opérations. □

L'unicité permet de parler *du* complété d'un corps valué. Celui-ci coïncide bien avec la notion usuelle de complété pour un espace métrique. On aurait d'ailleurs pu en réalité esquiver la majeure partie de la preuve en considérant le fait que $(K, |\cdot|)$ étant un espace métrique, il possède un complété unique à isométrie près, puis vérifier que celui-ci est bien muni d'une structure de corps valué en faisant passer à la limite les divers opérations pour les définir sur le complété.

Grâce au théorème précédent, on peut maintenant considéré le complété de $\mathbb{Q}$ par rapport à ses différentes valeurs absolues. Pour la valeur absolue usuelle, il s'agit de $\mathbb{R}$. Pour les valeurs absolues p-adique, on dispose de la définition suivante.

Définition 1.17. *Soit p un nombre premier. Le complété du corps valué $(\mathbb{Q}, |\cdot|_p)$ est appelé corps des nombres p-adiques et est noté $\mathbb{Q}_p$.*

1.3 Espaces vectoriels normés sur un corps valué complet

Cette section a pour objectif d'étendre la notion d'espace vectoriel normé à des corps plus variés que $\mathbb{R}$ ou $\mathbb{C}$, et de voir quelles propriétés usuelles se généralisent et sous quelles conditions.

1.3.1 Normes sur un espace vectoriel et équivalence de normes

Définition 1.18 (Espace vectoriel normé sur un corps valué)**.** *Soit $(K, |\cdot|)$ un espace vectoriel normé est la donné $(E, ||\cdot||)$ d'un K-espace vectoriel E et d'une application $||\cdot|| : E \to \mathbb{R}_+$ appelée norme et vérifiant les axiomes suivants :*

(i) $\forall x \in E, ||x|| = 0 \Leftrightarrow x = 0$ *(séparation) ;*

(ii) $\forall \lambda \in K \forall x \in E, ||\lambda x|| = |\lambda| ||x||$ *(homogénéité) ;*

(iii) $\forall x, y \in E, ||x + y|| \leq ||x|| + ||y||$ *(inégalité triangulaire).*

Donnons quelques exemples :

- Soit $(K, |\cdot|)$ un corps valué. La formules suivantes définissent des normes sur K^n :

$$||x||_\infty = \sup\{|x_i|, i \in [\![1, n]\!]\};$$
$$||x||_p = \left(\sum_{i=1}^{n} |x_i|^p\right)^{1/p} \text{ pour tout } p \geq 1$$

- Plus généralement, étant donné une base $\mathcal{B} = (e_1, \ldots, e_n)$ d'un espace vectoriel de dimension n sur un corps valué $(K, |\cdot|)$. Soit $x \in K$, en écrivant $x = \sum_{i=1}^{n} x_i e_i$ où $x_i \in K$. On peut définir les normes $||\cdot||_{p,\mathcal{B}}$ sur E pour $p \in [1, \infty]$ par les mêmes formules que dans l'exemple précédent.

- Soit $(L, |\cdot|)$ un corps valué et K un sous-corps de L. Alors $(L, |\cdot|)$ est un $(K, |\cdot|)$ espace vectoriel normé.

Comme usuellement, on peut alors définir les notions de boules ouvertes et de boules fermées et munir ainsi E d'une structure d'espace métrique. Ensuite, se pose la question de s'il est possible de généraliser les énoncés concernant l'équivalence des normes.

Définition 1.19 (Normes équivalentes)**.** *Soit E un espace vectoriel sur un corps valué $(K, |\cdot|)$ et deux normes $||\cdot||_1$, $||\cdot||_2$ sur E.*

- *$||\cdot||_1$ est dite plus fine que $||\cdot||_2$ s'il existe $a > 0$ tel que $\forall x \in E, ||x||_2 \leq a||x||_1$.*
- *$||\cdot||_1$ est dite moins fine que $||\cdot||_2$ s'il existe $b > 0$ tel que $\forall x \in E, b||x||_1 \leq ||x||_2$.*
- *$||\cdot||_1$ et $||\cdot||_2$ sont dites équivalentes si $||\cdot||_1$ est à la fois plus fine et moins fine que $||\cdot||_2$.*

Proposition 1.20. *Soit E un espace vectoriel sur un corps valué $(K, |\cdot|)$ et deux normes $||\cdot||_1$, $||\cdot||_2$ sur E. Alors $||\cdot||_1$ est plus fine (resp. moins fine) que $||\cdot||_2$ si et seulement si la topologie induite par $||\cdot||_1$ sur E est plus fine (resp. moins fine) que celle induite par $||\cdot||_2$. En particulier, $||\cdot||_1$ et $||\cdot||_2$ induisent la même topologie sur E si et seulement si elles sont équivalentes.*

Démonstration. Montrons le premier point. Le reste en découle. Soit $a > 0$ tel que $\forall x \in E, ||x||_2 \leq a||x||_1$. Soit U un ouvert de $(E, ||\cdot||_2)$. Soit $x \in U$. Comme U est ouvert, il existe $r > 0$ tel que $B_{||\cdot||_2}(x, r) \subset U$. Comme $\forall x \in E, ||x||_2 \leq a||x||_1$, on a $B_{||\cdot||_1}(x, \frac{r}{a}) \subset B_{||\cdot||_2}(x, \frac{r}{a})$. Ainsi, $B_{||\cdot||_2}(x, \frac{r}{a}) \subset U$ et donc U est un ouvert de $(E, ||\cdot||_1)$.

Réciproquement, si la topologie induite par $||\cdot||_1$ est plus fine que celle induite par $||\cdot||_2$ alors $B_{||\cdot||_2}(0, 1)$ étant un ouvert de $(E, ||\cdot||_2)$, c'est un ouvert de $(E, ||\cdot||_1)$. En particulier, 0 lui est intérieur et il existe donc $r > 0$ tel que $B_{||\cdot||_1}(0, r) \subset B_{||\cdot||_2}(0, 1)$. En particulier, $\forall x \in E, ||x||_1 < r \Rightarrow ||x||_2 < 1$. Soit $x \in E \backslash \{0\}$ et $0 < a < r$. On a $||\frac{ax}{||x||_1}||_1 < r$, donc $||\frac{ax}{||x||_1}||_2 < 1$ puis $||x||_2 < \frac{1}{a}||x||_1$ et donc $||\cdot||_1$ est plus fine que $||\cdot||_2$. □

Pour un espace vectoriel E de dimension finie sur n'importe quel corps normé K une norme $||\cdot||_{\infty,\mathcal{B}}$ est plus fine que n'importe quelle autre norme. En effet, en prenant $\mathcal{B} = (e_1, \dots, e_n)$ et $x = \sum_{i=1}^{n} x_i e_i \in E$, on a pour n'importe quelle norme $||\cdot||$ sur E, $||x|| \leq \sum_{i=1}^{n} |x_i|||e_i|| \leq \sum_{i=1}^{n} ||x||_{\infty,\mathcal{B}}||e_i|| \leq \left(\sum_{i=1}^{n} ||e_i||\right)||x||_{\infty,\mathcal{B}}$.

Toutefois, en général sur un espace vectoriel de dimension finie sur un corps valué, une norme n'est pas nécessairement plus fine que la norme $||\cdot||_{\infty,\mathcal{B}}$. Par exemple, en considérant $\mathbb{Q}$ munit de la valeur absolue usuelle et le $\mathbb{Q}$ espace vectoriel $\mathbb{Q}^2$, on définit une norme sur $\mathbb{Q}^2$ via $||(x_1, x_2)|| = |x_1 + x_2\sqrt{2}|$ où $|\cdot|$ est la valeur absolue usuelle sur $\mathbb{R}$. Cette norme n'est pas plus fine que $||\cdot||_\infty$. En effet, si $(x_n)_{n\in\mathbb{N}}$ est une suite de rationnels tendant vers $\sqrt{2}$, la suite $((x_n, -1))_{n\in\mathbb{N}}$ tend vers 0 dans $(\mathbb{Q}^2, ||\cdot||)$, mais pas dans $(\mathbb{Q}^2, ||\cdot||_\infty)$.

Pour remédier à cela, on impose de plus que $(K, |\cdot|)$ soit complet.

Proposition 1.21 (Équivalence des normes)**.** *Soit $(K, |\cdot|)$ un corps valué complet et E un K espace vectoriel de dimension finie, alors toutes les normes sur E sont équivalentes.*

Démonstration. La preuve suivante (tirée de [12, p.19]) va montrer le résultat par récurrence sur la dimension d de l'espace vectoriel E. Si $d = 1$, le résultat est immédiat. Soit E un espace vectoriel de dimension finie d sur K et $\mathcal{B} = (e_1, \dots, e_d)$ une base de E. Il suffit de montrer que toute norme $||\cdot||$ sur E est équivalente à $||\cdot||_{\infty,\mathcal{B}}$. On a déjà vu que $||\cdot||_{\infty,\mathcal{B}}$ est plus fine que $||\cdot||$. Montrons réciproquement que $||\cdot||$ est plus fine que $||\cdot||_{\infty,\mathcal{B}}$.

Si ce n'est pas la cas, il existe des suites $\left(x_1^{(n)}\right)_{n\in\mathbb{N}}, \dots, \left(x_d^{(n)}\right)_{n\in\mathbb{N}}$ telle qu'en posant $y_n = x_1^{(n)} e_1 + \cdots + x_d^{(n)} e_d$ pour tout $n \in \mathbb{N}$, la suite $(y_n)_{n\in\mathbb{N}}$ tende vers 0 pour $||\cdot||$, mais pas pour $||\cdot||_{\infty,\mathcal{B}}$. Ainsi, une des suites $\left(x_k^{(n)}\right)_{n\in\mathbb{N}}$ ne tend pas vers 0, et quitte à supposer qu'il s'agit de la première et à extraire, il existe $C > 0$ tel que $\forall n \in \mathbb{N}, |x_1^{(n)}| \geq C$. Ainsi, $\left(\frac{y_n}{x_1^{(n)}}\right)_{n\in\mathbb{N}}$ tend toujours vers 0 pour $||\cdot||$. Ainsi, $\frac{x_2^{(n)}}{x_1^{(n)}} e_2 + \cdots + \frac{x_d^{(n)}}{x_1^{(n)}} e_d \xrightarrow[n\to+\infty]{} -e_1$. Or $F = Vect(e_2, \dots, e_n)$ est un espace vectoriel de dimension $d-1$. En particulier, par hypothèse de récurrence, $||\cdot||$ équivaut à $||\cdot||_{\infty,(e_2,\dots,e_d)}$ sur F et définit donc la même topologie que cette dernière, qui correspond à la topologie produit sur K^{d-1}, ainsi F est complet comme produit fini de complets. En particulier, F est fermé et donc $-e_1 \in F$, ce qui est absurde. □

Finalement, on aura besoin de la proposition suivante caractérisant le complété d'une extension de corps.

Proposition 1.22. *Soit $(K, |\cdot|)$ un corps valué. Soit et $(L, |\cdot|)$ une extension finie de K contenue dans $\widehat{\overline{K}}$. Alors le complété de L est $L\widehat{K}$.*

Démonstration. En effet, $L\widehat{K}$ est de dimension finie sur $\widehat{K}$ donc est complet. De plus, l'adhérence de L dans $L\widehat{K}$ contient $\widehat{K}$ (qui est l'adhérence de K) et L, donc $L\widehat{K}$ et L est donc dense dans $L\widehat{K}$, ce qui montre le résultat. □

1.3.2 Séries sur un espace vectoriel normé

Les notions de séries et de convergence de ces dernières sur un corps valué ou un espace vectoriel sur un tel corps se définissent de la même façon qu'usuellement, que ce soit dans les corps normés ou les espaces vectoriels normés. La première notion qui demande un peu d'application pour être adaptée est celle de convergence absolue. Le cadre permettant de généraliser cette notion est celui des espaces de Banach.

Définition 1.23. *Soit $(K, |\cdot|)$ un corps valué. Un espace vectoriel normé $(E, ||\cdot||)$ est qualifié d'espace de Banach si la topologie induite par $||\cdot||$ sur E en fait un espace métrique complet.*

On a par exemple vu lors de la preuve de l'équivalence des normes qu'un espace vectoriel de dimension finie sur un corps complet est un espace de Banach.

Définition 1.24 (Convergence absolue)**.** *Soit $(E, ||\cdot||)$ un espace de Banach sur un corps valué $(K, |\cdot|)$. Soit $\sum x_n$ une série sur $(E, ||\cdot||)$. On dit que $\sum x_n$ converge absolument si $\sum ||x_n||$ converge.*

Proposition 1.25. *Soit $(E, ||\cdot||)$ un espace de Banach sur un corps valué $(K, |\cdot|)$. Si une série converge absolument, elle est convergente.*

Démonstration. Soit $\sum x_n$ une série absolument convergente. Soient $p \leq q$, on a

$$\left|\left|\sum_{n=0}^{q} x_n - \sum_{n=0}^{p} x_n\right|\right| = \left|\left|\sum_{n=p+1}^{q} x_n\right|\right| \leq \sum_{n=p+1}^{q} ||x_n|| \leq \sum_{n=p+1}^{+\infty} ||x_n|| \xrightarrow[p\to+\infty]{} 0.$$

Ceci montre que $\left(\sum_{n=0}^{p} x_n\right)_{p\in\mathbb{N}}$ est de Cauchy, donc convergente comme E est complet. □

Finissons par un résultat qui montre à quel point l'étude des séries sur un corps ultramétrique diffère du cas réel (ou complexe).

Proposition 1.26. *Soit $(K, |\cdot|)$ un corps valué complet ultramétrique. Une série à valeur dans K est convergente si et seulement si son terme général tend vers 0.*

Démonstration. Le sens direct est évident. Réciproquement, si (x_n) tend vers 0, pour tout $\varepsilon > 0$, on peut prendre $N \in \mathbb{N}$ tel que pour tout $n \geq N$, $|x_n| \leq \varepsilon$. Soient $q \geq p \geq N$, on a alors :

$$\left|\sum_{n=0}^{q} x_n - \sum_{n=0}^{p} x_n\right| = \left|\sum_{n=p+1}^{q} x_n\right| \leq \max\{|x_n|, n \in [\![p+1, q]\!]\} \leq \varepsilon.$$

Ceci montre que $\left(\sum_{n=0}^{p} x_n\right)_{p\in\mathbb{N}}$ est de Cauchy, donc convergente comme K est complet. □

2 Corps ultramétriques

On s'intéresse plus particulièrement dans cette seconde section aux spécificités des corps valués ultramétriques. Quand on parlera de corps ultramétrique par la suite, la valeur absolue ultramétrique considérée sera non triviale.

Comme on l'a vu lors de la définition de valuation, à une valeur absolue ultramétrique $|\cdot|$ sur un corps K on peut associer une valuation $v(\cdot) = -\ln(|\cdot|)$. On qualifiera celle-ci de valuation du corps K et on la notera v (où v_K s'il faut insister sur le corps). Il sera par moments plus pratique de faire appel à cette valuation plutôt qu'à la valeur absolue sur K.

2.1 Anneau des entiers

Soit $(K, |\cdot|)$ un corps ultramétrique, de par l'inégalité ultramétrique, la boule unité fermée de K est stable par addition. De plus, elle contient 1 et -1 et la multiplicativité de $|\cdot|$ la rend également stable par multiplication. Ceci justifie la définition suivante.

Définition 2.1. *Le sous anneau $\mathcal{O}_K = \{x \in K, |x| \leq 1\}$ de K est appelé anneau des entiers de K.*

On remarque ensuite que l'ensemble $m_K = \{x \in K, |x| < 1\}$ de K est un idéal de $\mathcal{O}_K$. Comme $|\cdot|$ est non trivial, $\mathcal{O}_K$ est un sous anneau strict de K et m_K un idéal propre de $\mathcal{O}_K$.

Définition 2.2 (Anneau local)**.** *Un anneau local est un anneau commutatif possédant un unique idéal maximal.*

Proposition 2.3. *$\mathcal{O}_K$ est un anneau local d'idéal maximal m_K.*

Démonstration. Soit $x \in \mathcal{O}_K \backslash \{0\}$. Si $|x| = 1$, alors $|x^{-1}| = 1$ et donc $x^{-1} \in O_K$ et si $|x| < 1$, $|x^{-1}| > 1$ et donc $x^{-1} \notin O_K$. Ainsi, m_K est l'ensemble des éléments non inversible de $\mathcal{O}_K$, ce qui montre qu'il contient tout idéal maximal. Comme il est propre, c'est donc le seul idéal maximal de $\mathcal{O}_K$. □

Comme m_K est maximal de $\mathcal{O}_K$, le quotient de $\mathcal{O}_K$ par m_K est un corps. Cet objet jouera un rôle important dans l'étude des corps ultramétriques.

Définition 2.4 (Corps résiduel)**.** *Le corps $k_K := \mathcal{O}_K/m_K$ est appelé corps résiduel de K.*

Proposition 2.5. *Soit $(K, |\cdot|)$ un corps ultramétrique et $\widehat{K}$ son complété. On a $k_{\widehat{K}} \simeq k_K$.*

Démonstration. Comme le noyau de la flèche naturel de $\mathcal{O}_K$ dans $\mathcal{O}_{\widehat{K}}/m_{\widehat{K}}$ est $m_{\widehat{K}} \cap K = m_K$, on a une injection i de $\mathcal{O}_K/m_K$ dans $\mathcal{O}_{\widehat{K}}/m_{\widehat{K}}$. Soit maintenant $x \in \mathcal{O}_{\widehat{K}}$. Comme K est dense dans K, il existe $y \in K$ tel que $x - y \in B(0,1) = m_K$, ce qui montre que $i(y + m_K) = x + m_{\widehat{K}}$ et donc la surjectivité de i. □

Définition 2.6 (Uniformisante)**.** *Soit K un corps ultramétrique dont la valuation est discrète. Un élément $p \in \mathcal{O}_K$ de valuation strictement positive minimale, sera qualifié d'uniformisante.*

Proposition 2.7. *Soit K un corps muni d'une valuation discrète. Son anneau des entiers $\mathcal{O}_K$ est principal et si p est une uniformisante, tout élément de $K^\times$ s'écrit de façon unique sous la forme up^n avec $n \in \mathbb{Z}$ et $u \in \mathcal{O}_K^\times$.*

Démonstration. Soit I un idéal de A non réduit à $\{0\}$. Comme v est discrète et que $v(\mathcal{O}_K) \subset \mathbb{R}_+$, on peut prendre $x \in I$ de valuation minimale. Soit maintenant $y \in I$. Comme x est de valuation minimale, $v(x^{-1}y) = v(y) - v(x) \geq 0$ donc $x^{-1}y \in \mathcal{O}_K$ et donc x divise y dans $\mathcal{O}_K$, ce qui montre $I \subset x\mathcal{O}_K$. L'inclusion réciproque étant évidente, $I = x\mathcal{O}_K$ est principal.

Comme il est principal, il est également factoriel. De plus, l'unique idéal maximal de $\mathcal{O}_K$ étant m_K, un élément qui engendre m_K est à association près le seul premier de $\mathcal{O}_K$. Or au vu du raisonnement précédent, un élément engendre m_K si et seulement si c'est une uniformisante. Le théorème de décomposition en produit de facteurs premiers dans un anneau factoriel permet alors de conclure. □

On s'intéresse maintenant à la forme prise par les notions qui précèdent dans le cas de $\mathbb{Q}_p$.

Définition 2.8 (Entiers p-adiques)**.** *L'anneau des entiers de $\mathbb{Q}_p$ est noté $\mathbb{Z}_p$. On l'appelle anneau des entiers p-adiques.*

p est une uniformisante de $\mathbb{Z}_p$ et l'idéal maximal de $\mathbb{Z}_p$ est donc $p\mathbb{Z}_p$. Enfin, par la proposition 2.5, $k_{\mathbb{Q}_p} \simeq k_{\mathbb{Q}}$. Or quand $\mathbb{Q}$ est muni de la topologie p-adique, son anneau des entiers est $\mathbb{Z}_{(p)}$, le localisé de $\mathbb{Z}$ en p, d'idéal maximal $p\mathbb{Z}_{(p)}$. Comme $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p\mathbb{Z}$, on a donc $k_{\mathbb{Q}_p} \simeq \mathbb{F}_p$.

2.2 Topologie ultramétrique

L'objectif de cette section est de considérer les spécificités d'une topologie ultramétrique sur un corps ultramétrique $(K, |\cdot|)$. Les propriétés suivantes nous donnent un premier exemple de situation qui diffère du cas des corps archimédiens. Elles sont tirées de [8, section 2.3].

Proposition 2.9. *Soit $(K, |\cdot|)$ un corps ultramétrique. Soient $x, y \in K$. Si $|x| \neq |y|$, alors $|x + y| = \max(|x|, |y|)$.*

Démonstration. Supposons $|x| > |y|$. Alors $|x + y| \leq \max(|x|, |y|) = |x|$. De plus, si $|x+y| < |x|$, $|x| = |(-y) + (x - y)| \leq \max(|x+y|, |-y|) < |x|$, ce qui est absurde. Ainsi, $|x + y| = |x| = \max(|x|, |y|)$. □

De façon équivalente, si v est la valuation de $(K, |\cdot|)$ et que $v(x) \neq v(y)$, $v(x+y) = \min(v(x), v(y))$.

On en déduit le corollaire suivant.

Corollaire 2.10 (Tous les triangles sont isocèles)**.** *Soit $(K, |\cdot|)$ un corps ultramétrique. Soient $x, y, z \in K$. Parmi $d(x,y), d(x,z)$ et $d(y,z)$, au moins deux sont égaux. De plus, la troisième longueur est moins longue que les deux autres (non nécessairement strictement).*

Démonstration. Si $d(x,y) \neq d(x,z)$, alors $|x-y| \neq |z-x|$ et donc $d(y,z) = |z-y| = |(x-y)+(z-x)| = \max(|x-y|, |z-x|) = \max(d(x,z), d(y,x))$. Dans le cas ci dessus, ceci montre que le côté le plus petit est moins long. Si maintenant $d(x,y) = d(x,z)$, l'inégalité triangulaire montre que $d(y,z) \leq d(x,z)$. □

Cette propriété a un certain nombre de conséquences intéressantes concernant la topologie des boules ouvertes et fermées.

Proposition 2.11. *Dans un corps ultramétrique, tout point d'une boule ouverte ou fermée en est le centre.*

Démonstration. Montrons le dans le cas d'une boule ouverte. soient $x \in K$, $r > 0$ et $y \in B(x,r)$. Soit $z \in B(x,r)$, on a $d(z,y) \leq \max(d(x,y), d(y,z))$ donc $z \in B(y,r)$, d'où $B(x,r) \subset B(y,r)$. On obtient l'autre inclusion en inversant les rôles de x et y. □

On en déduit en particulier que dans un corps ultramétriques, deux boules sont ou bien disjointes, ou bien contenues l'une dans l'autre.

Ceci va amener des propriétés topologiques assez inhabituelles pour les corps ultramétriques. Pour décrire celles-ci on va avoir besoin de la définition suivante, adaptée de l'anglais "clopen".

Définition 2.12 (Partie fouverte)**.** *Une partie d'un espace topologique à la fois ouverte et fermée sera dite fouverte.*

Proposition 2.13. *Les boules ouvertes et les boules fermées de rayon non nul sont des parties fouvertes d'un corps ultramétrique.*

Démonstration. Une boule fermée est fermée par définition. Soient $x \in K$ et $r > 0$. Si $y \in \overline{B}(x,r)$ avec $r > 0$, on a $\overline{B}(y,r) = \overline{B}(x,r)$ par la proposition précédente, donc $B(y,r) \subset \overline{B}(x,r)$, ce qui montre que $\overline{B}(x,r)$ est ouverte.

Une boule ouverte est ouvert par définition. Soient $x \in K$ et $r > 0$. Montrons que $B(x,r)$ est ouverte en montrant que son complémentaire est fermé. Soit $z \in K$ tel que $d(z,x) \geq r$. Soit $y \in B(z,r)$. Comme $d(y,z) < r \leq d(z,x)$, par "tous les triangles sont isocèles", $d(y,x) = d(z,x) \geq r$ et donc $B(z,r)$ est incluse dans le complémentaire de $B(x,r)$, ce qui montre que $B(x,r)$ est fermée. □

Comme $\mathcal{O}_K$ et m_K sont respectivement les boules unités ouvertes et fermées, ce sont donc des fouverts de K.

Corollaire 2.14. *Les composantes connexes d'un corps ultramétrique sont ses singletons.*

Démonstration. Soit $x \in K$ et C sa composante connexe. Supposons qu'il existe $y \in C \backslash \{x\}$. Soit $r = d(x,y)$. Alors $B(x,r) \cap C$ est un fouvert non trivial de C, ce qui est absurde car C est connexe. Ainsi, $C = \{x\}$. □

Donnons enfin une dernière définition que l'on pourra notamment appliquer par la suite au corps des nombres p-adiques.

Définition 2.15 (Corps local)**.** *Un corps valué muni d'une valeur absolue non triviale est dit local s'il est localement compact.*

Notons que par localement compact, on entend que chaque point admet un voisinage compact. En particulier, on sait déjà comme conséquence du théorème de Bolzano-Weierstrass que les corps $\mathbb{R}$ et $\mathbb{C}$ sont localement compacts. En réalité, être localement compact revient à vérifier la propriété de Bolzano-Weierstrass comme le montre la proposition suivante.

Proposition 2.16. *Soit $(K, |\cdot|)$ un corps local. Les parties compactes de K sont les fermés bornés de K.*

Démonstration. Comme dans le cas réel, un compact est fermé et borné. Réciproquement, comme K est localement compact, il existe un voisinage compact V de 0. Soit $\varepsilon > 0$ tel que $\overline{B}(0,\varepsilon) \subset V$. $\overline{B}(0,\varepsilon)$ est un fermé de V donc est compacte. Alors $\bigcup_{x\in\overline{B}(0,\varepsilon)} B(x, \frac{\varepsilon}{2})$ est un recouvrement du compact $\overline{B}(0,\varepsilon)$ par des ouverts. Il existe donc $x_1, \dots x_n \in K$ tels que $\overline{B}(0,\varepsilon) \subset \bigcup_{i=1}^{n} B(x_i, \frac{\varepsilon}{2})$, puis

$$\overline{B}(0, \frac{3}{2}\varepsilon) \subset \bigcup_{i=1}^{n} B(x,\varepsilon) \subset \bigcup_{i=1}^{n} \overline{B}(x,\varepsilon).$$

Ce dernier ensemble est une union finie de compacts, donc est compact et $\overline{B}(0, \frac{3}{2}\varepsilon)$ en étant un fermé, il est également compact. Par récurrence, on en déduit que pour tout $n \in \mathbb{N}$, $\overline{B}(0, \left(\frac{3}{2}\right)^n \varepsilon)$ est compact. Soit maintenant F un fermé borné de K, il est inclus dans $\overline{B}(0, \left(\frac{3}{2}\right)^n \varepsilon)$ pour n assez grand. C'est donc un compact en tant que partie fermée d'un compact. □

Nous pouvons maintenant donner une caractérisation des corps ultramétriques locaux tirée de [5, p.50].

Proposition 2.17. *Soit $(K, |\cdot|)$ un corps local ultramétrique. K est complet, sa valuation est discrète et k_K est fini.*

Démonstration. Supposons K local. Soit $(x_n)_{n\in\mathbb{N}}$ une suite de Cauchy. $(x_n)_{n\in\mathbb{N}}$ est bornée et K localement compact, donc par la proposition précédente, elle admet une valeur d'adhérence. Comme une suite de Cauchy admettant une valeur d'adhérence converge vers celle-ci, K est complet.

Montrons maintenant que $-\ln(|\cdot|)$ est discrète. Comme m_K est un fermé borné de K, il est compact. Ainsi, l'image de m_K par $-\ln(|\cdot|)$ est un compact de $\mathbb{R}_+ \cup \{\infty\}$ donc est une partie minorée de $\mathbb{R}_+$, ce qui montrer que $-\ln(|\cdot|)$ est discrète.

Finalement, soit $(x_i)_{i\in I}$ un ensemble de représentant des éléments de k_K dans $\mathcal{O}_K$. Alors $\bigcup_{i\in I} B(x_i,1)$ est un recouvrement d'ouverts de $\mathcal{O}_K$ qui est compact, donc il existe $i_1,\dots,i_n$ tel que $\mathcal{O}_K \subset \bigcup_{k=1}^{n} B(x_{i_k},1)$, c'est à dire $m_K \subset \{\pi(x_{i_1}),\dots,\pi(x_{i_1})\}$ avec π la projection canonique, et donc k_K est fini. □

2.3 Développement de Hensel

Dans le cas d'un corps muni d'une valuation discrète on dispose d'une écriture "en base p" des éléments de $\mathcal{O}_K$.

Proposition 2.18 (Développement de Hensel)**.** *Soit $(K,|\cdot|)$ un corps ultramétrique complet dont la valuation est discrète. Soit p une uniformisante. Soit $R \subset \mathcal{O}_K$ un ensemble de réprésentants de k_K. Alors, l'application*

$$\begin{cases} R^{\mathbb{N}} \to \mathcal{O}_K \\ (x_n)_{n\in\mathbb{N}} \mapsto \sum_{n=0}^{\infty} x_n p^n \end{cases}$$

est une bijection.

Démonstration. L'application est bien définie car K est complet et le terme général de la série tend vers 0. De plus, si $\sum_{n=0}^{\infty} x_n p^n = \sum_{n=0}^{\infty} x'_n p^n$, en réduisant modulo p, on trouve $x_0 = x'_0$, puis après simplification par p, on peut réitérer le processus et déduire que pour tout $n \in \mathbb{N}$, $x_n = x'_n$. Montrons enfin la surjectivité de l'application. Soit $x \in \mathcal{O}_K$. On définit la suite (x_n) par récurrence en prenant : x_0 est l'unique élément de R tel que $x \equiv x_0 \bmod p\mathcal{O}_K$ et x_n l'unique élément de R tel que $x_n \equiv p^{-n}\left(x - \sum_{k=0}^{n-1} x_k p^k\right) \bmod p\mathcal{O}_K$. Par construction, on a $x \equiv \sum_{k=0}^{n-1} x_k p^k \bmod p^n\mathcal{O}_K$, c'est à dire $\left|x - \sum_{k=0}^{n-1} x_k p^k\right| \leq |p|^k$. Comme p est une uniformisante, $|p|<1$ et on a donc bien $x = \sum_{k=0}^{+\infty} x_k p^k$. □

On peut alors étendre la notion d'écriture en base p à tout élément de K en constatant que $p^n x \in \mathcal{O}_K$ pour n assez grand. Ainsi, l'écriture d'un élément de $K\backslash\mathcal{O}_K$ fait intervenir des puissances négatives de p.

Proposition 2.19. *Soit K un corps ultramétrique complet dont la valuation est discrète et le corps résiduel est fini. Alors $\mathcal{O}_K$ est compact.*

Démonstration. Soit $(U_i)_{i\in I}$ une famille d'ouverts recouvrant $\mathcal{O}_K$. Soit p une uniformisante et R un ensemble de représentants de k_K. Supposons qu'aucune sous-famille finie de $(U_i)_{i\in I}$ ne recouvre $\mathcal{O}_K$ alors comme $\mathcal{O}_K = \bigcup_{x\in R}(x+p\mathcal{O}_K)$, il existe $x_0 \in R$ tel qu'aucune sous-famille finie de $(U_i)_{i\in I}$ ne recouvre $x_0 + p\mathcal{O}_K$. De même, en écrivant $x_0 + p\mathcal{O}_K = \bigcup_{x\in R}(x_0 + xp + p^2\mathcal{O}_K)$, on en déduit l'existence de x_1 telle qu'aucune

sous-famille finie de $(U_i)_{i\in I}$ ne recouvre $x_0 + x_1 p + p^2\mathcal{O}_K$. En réitérant le processus, on construit une suite $(x_n)_{n\in\mathbb{N}}$ telle qu'aucune sous-famille finie de $(U_i)_{i\in I}$ ne recouvre $x_0 + x_1 p + ... + x_n p^n + p^{n+1}\mathcal{O}_K$. Soit $x = \sum_{n=0}^{\infty} x_n p^n$. Il existe $i \in I$ tel que $x \in U_i$. Comme U_i est ouvert, il existe $r > 0$ tel que $B(x, r) \subset U_i$ et donc pour n suffisament grand, $x + p^n\mathcal{O}_K \subset U_i$ et donc $x_0 + x_1 p + ... + x_{n-1}p^{n-1} + p^n\mathcal{O}_K \subset x + p^n\mathcal{O}_K \subset U_i$, ce qui donne la contradiction que l'on souhaitait. □

On en déduit la réciproque de la proposition 2.17.

Corollaire 2.20. *Soit K un corps ultramétrique complet dont la valuation est discrète et le corps résiduel est fini. Alors K est un corps local.*

Démonstration. On vient de voir que sous ces hypothèses, $\mathcal{O}_K$ est compact. Comme il est de plus ouvert, il s'agit d'un voisinage compact de 0. Par translation, on en déduit que pour tout $x \in K$, $x + \mathcal{O}_K$ est un voisinage compact de $\mathcal{O}_K$. Ainsi, K est localement compact. □

Proposition 2.21. *Soit $(K, |\cdot|)$ un corps ultramétrique, de corps résiduel fini et dont la valuation est discrète. Alors $(\widehat{K}, |\cdot|)$ est un corps local.*

Démonstration. $\widehat{K}$ est complet par définition. Comme $v(K) = a\mathbb{Z}$ pour un $a \in \mathbb{R}_+$, K est dense dans $\widehat{K}$ et que v est continue, $v(\widehat{K}) = a\mathbb{Z}$, ce qui montre que la valuation de $\widehat{K}$ est discrète. Finalement, par la proposition 2.5, $k_{\widehat{K}}$ est fini. Par la proposition 2.20, $\widehat{K}$ est local. □

En appliquant le résultat précédent à $(\mathbb{Q}, |\cdot|_p)$, on obtient le résultat suivant.

Corollaire 2.22. *Soit p un nombre premier. Le corps des nombres p-adiques $\mathbb{Q}_p$ est un corps local.*

On déduit alors de la proposition 2.18, l'écriture canonique en base p dans $\mathbb{Q}_p$.

Proposition 2.23 (Développement de Hensel dans $\mathbb{Q}_p$)**.** *Tout élément $x \in \mathbb{Q}_p$ s'écrit de façon unique sous la forme $x = \sum_{n=v_p(x)}^{+\infty} a_n p^n$ avec les a_n dans $[\![0, p-1]\!]$ et $a_0 \neq 0$.*

Un autre exemple de corps local est donné par le corps des séries formelles sur $\mathbb{F}_q$ pour $q = p^n$. En effet, X est un polynôme irréductible de $\mathbb{F}_q[X]$ et on peut donc considérer la valuation X-adique $|\cdot|_X$ sur $\mathbb{F}_q(X)$. Le complété de $\mathbb{F}_q(X)$ pour $|\cdot|_X$ est alors noté $\mathbb{F}_q((X))$, le corps des séries formelles à coefficients dans $\mathbb{F}_q$. Son anneau des entiers est alors l'anneau des séries formelles $\mathbb{F}_q[[X]]$ et son corps résiduel est $\mathbb{F}_q$. Le développement de Hensel donne alors que les éléments de $\mathbb{F}_p((X))$ s'écrivent de façon unique $\sum_{n=r}^{+\infty} a_n X^n$ avec $r \in \mathbb{Z}$, les a_n des $\mathbb{F}_p$ et $a_0 \neq 0$, ce qui est bien la façon dont on voit usuellement les séries formelles.

2.4 Lemme de Hensel et carrés dans $\mathbb{Q}_p$

La proposition suivante va nous permettre de "relever" des solutions d'une équation polynomiale dans le corps résiduel d'un corps ultramétrique complet K en des solutions de cette même équation dans $\mathcal{O}_K$. Dans le cas de $\mathbb{Q}_p$, avec $p \geq 3$ on en déduira en particulier qu'un entier est un carré dans $\mathbb{Z}_p$ si et seulement si c'en est un dans $\mathbb{F}_p$.

Proposition 2.24 (Lemme d'Hensel)**.** *Soit K un corps local ultramétrique complet et $P \in \mathcal{O}_K[X]$. Soit $x \in \mathcal{O}_K$ tel que $|P(x)| < |P'(x)|^2$. Alors P admet une unique racine dans $B(x, |f'(x)|)$. De plus, la suite définie par récurrence par $x_0 = x$ et pour tout $n \in \mathbb{N}$, $x_{n+1} = x_n - \frac{P(x_n)}{P'(x_n)}$ converge vers cette racine.*

La preuve qui suit est issue de [12, p.15].

Démonstration. On note $c = \left|\frac{P(x)}{P'(x)^2}\right|$. Montrons par récurrence sur $n \in \mathbb{N}^*$ que x_{n+1} est bien défini, que $|P'(x_n)| = |P'(x)|$, $|x_{n+1} - x_n| \leq c^{2^n}|P'(x)|$ et $|P(x_n)| \leq c^{2^n}|P'(x)|^2$.

Comme $|P(x)| < |P'(x)|^2$, $P(x_0) \neq 0$ et x_1 est bien défini. De plus $|x_1 - x_0| = \left|\frac{P(x_0)}{P'(x_0)}\right| = c$ et $|P(x_0)| = |P(x)| = c|P'(x)|^2$.

Supposons le résultat au rang n et montrons le au rang $n+1$. En appliquant la formule de Taylor à l'ordre 1 à P' en x_n, on sait qu'il existe $s_n \in \mathcal{O}_K$ tel que

$$P'(x_{n+1}) = P'(x_n) + s(x_{n+1} - x_n) = P(x_n) + s\frac{P(x_n)}{P'(x_n)}.$$

Or

$$\left|s\frac{P(x_n)}{P'(x_n)}\right| \leq \frac{|P(x_n)|}{|P'(x_n)|} \leq \frac{c^{2^n}|P'(x)|^2}{|P'(x)|} < |P'(x)| = |P'(x_n)|,$$

donc par "tous les triangles sont isocèles", $|P'(x_{n+1})| = |P'(x_n)|$.

D'après la formule de Taylor polynomiale à l'ordre 2,

$$P(x_{n+1}) = P(x_n) + P'(x_n)(x_{n+1} - x_n) + r(x_n - x_{n+1})^2$$

pour un certain $r_n \in \mathcal{O}_K$. On a donc

$$P(x_{n+1}) = P(x_n) - P'(x_n)\frac{P(x_n)}{P'(x_n)} + r_n(x_{n+1} - x_n)^2 = r_n(x_{n+1} - x_n)^2.$$

Ainsi,

$$|P(x_{n+1})| \leq |x_{n+1} - x_n|^2 \leq (c^{2^n}|P'(x)|)^2 = c^{2^{n+1}}|P'(x)|^2.$$

On en déduit aussitôt

$$|x_{n+2} - x_{n+1}| = \frac{|P(x_{n+1})|}{|P'(x_{n+1})} = \frac{|P(x_{n+1})|}{|P'(x)|} \leq \frac{c^{2^{n+1}}|P'(x)|^2}{|P'(x)|} \leq c^{2^{n+1}}|P'(x)|.$$

La suite $(x_n)_{n\in\mathbb{N}}$ est de Cauchy. En effet, pour $m \geq n$, on a $|x_m - x_n| \leq \max\{|x_{k+1} - x_k|, k \in [\![n, m-1]\!]\} \leq c^{2^n}|P'(x)| \xrightarrow[n\to+\infty]{} 0$, car $c < 1$. Notons x_∞ la limite de cette

suite. En prenant $n = 0$ et en faisant tendre m vers l'infini dans la formule ci dessus, on a $x_\infty \in B(x, |P'(x)|)$. En passant à la limite dans l'inégalité $|P(x_n)| \leq c^{2^n}|P'(x)|^2$, on a $P(x_\infty) = 0$. De même, on obtient $|P'(x_\infty)| = |P'(x)|$ en passant à la limite dans $|P'(x_n)| = |P'(x)|$.

Montrons enfin l'unicité. Soit y une racine de P. On a

$$P(x_\infty) = P(y) + P'(x_\infty)(x_\infty - y) + a(x_\infty - y)^2$$

avec $a \in \mathcal{O}_K$. On a donc $P'(x_\infty) = -a(x_\infty - y)$, et donc $|x_\infty - y| \geq |P'(x_\infty)| = |P'(x_\infty)|$. □

Corollaire 2.25. *Soit K un corps ultramétrique complet. Soit $P \in \mathcal{O}_K[X]$. Si P admet une racine simple dans k_K alors P admet une racine dans $\mathcal{O}_K$.*

Démonstration. Soit $x \in \mathcal{O}_K$ dont la réduction modulo m_K est une racine simple de P dans k_K. On a $P(x) \in m_K$ et $P'(x) \in \mathcal{O}_K \backslash m_K$ d'où $|P(x)| < 1$ et $|P'(x)| = 1$. Ainsi $|P(x)| < |P'(x)|^2$. Les hypothèses du lemme de Hensel sont donc vérifiées et celui-ci permet de conclure. □

Dans le cas de $\mathbb{Q}_p$, le corps résiduel est $\mathbb{F}_p$. Ainsi, si $P \in \mathbb{Z}_p[X]$ admet une racine simple dans $\mathbb{F}_p$, il en admet une dans $\mathbb{Z}_p \subset \mathbb{Q}_p$. Si réciproquement P est un polynôme unitaire de $\mathbb{Z}_p[X]$ admettant une racine dans $\mathbb{Q}_p$, comme $\mathbb{Z}_p$ est factoriel, celle-ci est dans $\mathbb{Z}_p$ et on peut donc la réduire modulo $p\mathbb{Z}_p$ ce qui fait que P admet une racine dans $\mathbb{F}_p$. On va se servir de ces considérations et plus généralement, du lemme d'Hensel pour étudier les carrés de $\mathbb{Z}_p$.

Proposition 2.26. *Soit p un nombre premier. Soit $a \in \mathbb{Z}_p^\times$.*

- *Si p est impair alors a est un carré dans $\mathbb{Q}_p$ si et seulement si c'en est un dans $\mathbb{F}_p$.*
- *Si $p = 2$, alors a est un carré dans $\mathbb{Q}_2$ si et seulement si c'en est un dans $\mathbb{Z}_p/8\mathbb{Z}_p \simeq \mathbb{Z}/8\mathbb{Z}$.*

Démonstration. Soit p un nombre premier et $a \in \mathbb{Z}_p^\times$. Comme $\mathbb{Z}_p$ est factoriel, si $X^2 - a$ admet une racine dans $\mathbb{Q}_p$, celle-ci est dans $\mathbb{Z}_p$. Ainsi, en réduisant modulo $p\mathbb{Z}_p$ si p est impair (resp. modulo $8\mathbb{Z}_2$ si $p = 2$), $X^2 - a$ admet une racine dans $\mathbb{F}_p$ (resp. $\mathbb{Z}/8\mathbb{Z}$) et donc a est un carré dans $\mathbb{F}_p^\times$ (resp $\mathbb{Z}/8\mathbb{Z}^\times$).

Réciproquement, si p est impair et a est un carré dans $\mathbb{F}_p$, alors $P := X^2 - a$ admet une racine dans $\mathbb{F}_p$ et celle-ci est simple car comme $p \neq 2$, $X^2 - a$ est premier avec $P' = 2X$ donc à racines simples. Le corollaire précédent assure alors que $X^2 - a$ admet une racine dans $\mathbb{Z}_p$ et a est donc un carré dans $\mathbb{Q}_p$.

Finalement, si $p = 2$ et $P := X^2 - a$ admet une racine dans $\mathbb{Z}/8\mathbb{Z}$, on peut prendre $x \in \mathbb{Z}_2$ tel que $x^2 - a \in 8\mathbb{Z}_2$. On a alors $v_2(P(x)) \geq 3$ et $v_p(P'(x)) = v_2(2x) = v_2(2) + v_2(x) = 1$, d'où $|P(x)|_2 < |P'(x)|^2$. Le lemme d'Hensel s'applique alors et P admet une racine dans $\mathbb{Z}_2$ donc a est un carré dans $\mathbb{Q}_2$. □

2.5 Extension de valeurs absolues

Soit p un nombre premier. On va maintenant chercher à étendre la valeur absolue p-adique à la clôture algébrique de $\mathbb{Q}_p$, qu'on notera $\overline{\mathbb{Q}}_p$.

On commence par le résultat suivant, de portée plus générale.

Proposition 2.27. *Soient $(K, |\cdot|)$ un corps valué complet et L une extension finie de K. Alors il existe au plus une valeur absolue sur L prolongeant $|\cdot|$.*

Démonstration. $|\cdot|_1, |\cdot|_2$ étant des valeurs absolues sur L prolongeant K, ce sont en particulier des normes sur L en tant que $(K, |\cdot|)$-espace vectoriel normé. Comme K est complet et L de dimension finie, $|\cdot|_1, |\cdot|_2$ sont équivalentes en tant que normes, puis définissent la même topologie sur L et donc sont équivalentes en tant que valeur absolues. On distingue alors deux possibilités. Si $|\cdot|$ est triviale, alors $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes à la valeur absolue triviale sur L car celle-ci prolonge $|\cdot|$. Ainsi, $|\cdot|_1$ et $|\cdot|_2$ sont triviales et en particulier égales. Si maintenant $|\cdot|$ n'est pas triviale, comme $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes, on peut écrire $|\cdot|_1 = |\cdot|_2^s$ pour un certain $s > 0$. Mais alors, en évaluant l'égalité en un élément de $x \in K$ tel que $|x| \neq 1$, on obtient $s = 1$ et les deux valeurs absolues sont égales. □

On cherche à étendre la valeur absolue $|\cdot|_p$ à une extension finie de $\mathbb{Q}_p$. Pour cela, on va s'inspirer de l'extension de la valeur absolue usuelle $|\cdot|_\infty$ de $\mathbb{R}$ à $\mathbb{C}$. En effet, pour définir $|x|_\infty$ pour $x \in \mathbb{C}$, on pose $|x|_\infty = \sqrt{x\overline{x}}$. En réalité, la quantité $x\overline{x}$ a une signification algébrique importante : il fait intervenir les deux plongements de $\mathbb{C}$ dans lui-même fixant $\mathbb{R}$ à s'avoir l'identité et la conjugaison complexe, le produit de ces deux images d'un complexes par ces deux morphismes est ce qu'on appelle la norme de x : $N_{\mathbb{C}/\mathbb{R}}(x) = x\overline{x}$. Plus généralement, on peut définir la norme de n'importe quelle extension de corps de dimension finie.

Définition 2.28. *Soient L/K une extension finie séparable de degré n. Soient $\sigma_1, \ldots, \sigma_n$ les morphismes de K algébre de L dans sa clôture algébrique $\overline{L}$. Soit $x \in L$, on appelle norme de x dans L/K la quantité $N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x)$.*

La norme est multiplicative et c'est un exercice classique de théorie de Galois que de montrer qu'elle est à valeur dans K. De plus, on a pour tout $x \in L$, $N_{L/K}(x) = \det(m_x)$ où $m_x \in End_K(L)$ est la multiplication par x (cf. [4, p.147]).

Dans le cas de l'extension de la valeur absolue usuelle de $\mathbb{C}$ à $\mathbb{R}$, on a $|x|_\infty = \sqrt{N_{\mathbb{C}/\mathbb{R}}(x)}$. On s'en inspire pour prolonger une valeur absolue d'un corps local à une de ses extension finies.

Proposition 2.29. *Soit $(K, |\cdot|_K)$ un corps local ultramétrique et L une extension de degré n de K. Il existe un unique prolongement de $|\cdot|_K$ à L et celui-ci est donné par $\forall x \in L, |x|_L = \sqrt[n]{|N_{L/K}(x)|_K}$.*

Démonstration. L'unicité vient de la proposition 2.27. Pour l'existence, il suffit de vérifier que la formule précédente définit bien une valeur absolue prolongeant $|\cdot|_K$. La multiplicativité, la séparation et le fait que $|\cdot|_L$ prolonge $|\cdot|_K$ sont immédiats, la seule difficulté provient de l'inégalité ultramétrique. Pour cela, on montre que $|\cdot|_L$ vérifie l'inégalité triangulaire étendue pour une certaine constante C et donc qu'il s'agit d'une valeur absolue étendue. Le fait que sa restriction à K est ultramétrique permet alors de conclure qu'il s'agit bien d'une valeur absolue ultramétrique par la remarque suivant la proposition 1.8.

Soient $x, y \in L$. Il faut montrer qu'il existe $C > 0$ tel que $|x+y|_L \leq C \max(|x|_L, |y|_L)$. Supposons $|x|_L \geq |y|_L$, en divisant par $|x|_L$, il suffit donc de montrer $|1 + \frac{x}{y}|_L \leq C$ et donc que la fonction $z \mapsto |1+z|_L$ est bornée sur $\{z \in L, |z|_L \leq 1\}$.

Soit $\mathcal{B} = (e_1, ..., e_n)$ une base de L sur K. On munit L de la norme $||\cdot||_{\infty,\mathcal{B}}$. Comme $N_K(x) = \det(m_x)$ et que les coefficients de la matrices de m_x dans la base $\mathcal{B}$ sont linéaires en les cordonnées de x dans la base $\mathcal{B}$, par continuité du déterminant, on en déduit que N_K est continue pour $||\cdot||_{\infty,\mathcal{B}}$ et donc que $|\cdot|_L$ est continue vis à vis de $||\cdot||_{\infty,\mathcal{B}}$. Soit S la sphère unité de L pour $||\cdot||_{\infty,\mathcal{B}}$. Comme L est de dimension finie sur un corps local, S est compacte et comme $|\cdot|_L$ ne s'annule pas sur S, il existe donc $M, m > 0$ tel que $\forall y \in S, m \leq |y|_L \leq M$. Soit $x \in L^\times$, au vu de la définition de la norme infinie, il existe $\lambda \in K$ tel que $||x||_{\infty,\mathcal{B}} = |\lambda|_K$. On a alors $\frac{x}{\lambda} \in S$ et donc $m \leq |\frac{x}{\lambda}|_L \leq M$ et enfin $m||x||_{\infty,\mathcal{B}} \leq |x|_L \leq M||x||_{\infty,\mathcal{B}}$. En particulier, si $|z|_L \leq 1$, on a

$$\begin{aligned} |1+z| &\leq M||1+z||_{\infty,\mathcal{B}} \leq M(||1||_{\infty,\mathcal{B}} + ||z||_{\infty,\mathcal{B}}) \\ &\leq M(||1||_{\infty,\mathcal{B}} + m^{-1}|z|_L) \leq M(||1||_{\infty,\mathcal{B}} + m^{-1}), \end{aligned}$$

ce que l'on souhaitait. □

En réalité, dans le cas d'un corps local archimédien, la preuve montre également qu'il s'agit d'une valeur absolue étendue. Il suffirait alors de montrer que la constante d'une valeur absolue est invariante par passage au surcorps (ce qui est vrai : voir [4, p.78]) pour conclure.

Corollaire 2.30. *Soit $(K, |\cdot|)$ un corps local ultramétrique local et $\overline{K}$ sa clôture algébrique, $|\cdot|$ s'étend de façon unique à K.*

Démonstration. Montrons l'unicité. Soit $x \in \overline{K}$. Par la proposition précédente, il y a unicité d'une valeur absolue étendant $|\cdot|$ sur $K(x)$. En notant cette extension $|\cdot|_{K(x)}$, on a donc $|x|_{\overline{K}} = |x|_{K(x)}$.

Pour l'existence, la seule formule possible nous étant donnée par l'unicité, il s'agit juste de constater que si $x \in K_1, K_2 \subset \overline{K}$, on a $|x|_{K_1} = |x|_{K_2}$. Or, par la compatibilité de la norme au passage à une extension plus grande, on a bien $|x|_{K_1} = |x|_{K_1K_2} = |x|_{K_2}$. □

En particulier, les deux propositions précédentes s'appliquent dans le cas où $K = \mathbb{Q}_p$ et on a donc réussi à étendre $|\cdot|_p$ à la clôture algébrique de $\mathbb{Q}_p$.

3 Théorèmes d'Ostrowski

3.1 Théorème d'Ostrowski pour $\mathbb{Q}$

Nous avons jusqu'à maintenant exhibé trois familles de valeurs absolues sur $\mathbb{Q}$:

- La valeur absolue triviale.
- La valeur absolue usuelle que l'on notera $|\cdot|_\infty$ dans cette section.
- Pour chaque nombre premier p, la valeur absolue p-adique $|\cdot|_p$.

Le théorème d'Ostrowski pour $\mathbb{Q}$ énonce qu'il s'agit des seules valeurs absolues sur $\mathbb{Q}$ à équivalence près.

On commence par énoncer un résultat classifiant partiellement les valeurs absolues non-archimédiennes sur le corps des fractions d'un anneau principal qui nous permettra de classifier les valeurs absolues non archimédiennes sur $\mathbb{Q}$ et que l'on réutilisera également par la suite pour classifier les valeurs absolues sur $K[X]$. Ce résultat est tiré de [3].

Proposition 3.1. *Soit A un anneau principal et K son corps des fractions. Soit $|\cdot|$ une valeur absolue ultramétrique non triviale sur K telle que $\forall x \in A, |x| \leq 1$. Alors il existe un élément premier $p \in A$ tel que $|\cdot|$ soit une valeur absolue p-adique, c'est à dire de la forme $c^{v_p(\cdot)}$ avec $c \in]0,1[$.*

Démonstration. Comme $|\cdot|$ est non triviale, il existe $x \in A$ tel que $|x| < 1$. L'élément x n'est pas inversible dans A, sinon, on aurait $|x^{-1}| = |x|^{-1} > 1$, ce qui contredit l'hypothèse de la proposition. En décomposant x en produit de facteurs premiers, on en déduit qu'il existe un premier $p \in A$ tel que $|p| < 1$. On va montrer que $|\cdot| = c^{v_p(\cdot)}$ avec $c = |p|$.

Soit $x \in K$, on peut écrire $x = \frac{u}{v} p^{v_p(x)}$ avec $u, v \in A$ premiers avec p. On a donc $|x| = \frac{|u|}{|v|} c^{v_p(x)}$. Ainsi, il suffit de montrer que pour tout $y \in A$ premier avec p, $|y| = 1$. Comme y est premier avec p et que A est principal, par le théorème de Bézout, il existe $a, b \in A$ tel que $ap + by = 1$. Par l'inégalité ultramétrique, on obtient $1 = |1| \leq \max(|ap|, |by|)$ et comme $|ap| = |a||p| \leq c < 1$, on a $|by| \geq 1$ et comme $|b| \leq 1$, on a donc $|y| \geq 1$, d'où $|y| = 1$ comme $y \in A$. Ainsi, on a bien $|\cdot| = c^{v_p(\cdot)}$. □

On est maintenant en mesure de montrer le théorème d'Ostrowski pour $\mathbb{Q}$.

Théorème 3.2 (Théorème d'Ostrowski pour $\mathbb{Q}$)**.** *Toute valeur absolue sur $\mathbb{Q}$ est équivalente à une et une seule des valeurs absolues suivantes :*

- *La valeur absolue triviale.*
- *La valeur absolue usuelle $|\cdot|_\infty$.*
- *La valeur absolue p-adique $|\cdot|_p$ pour un nombre premier p donné.*

Démonstration. Montrons d'abord l'unicité. Il s'agit de prouver que les valeurs absolues ci-dessus sont non équivalentes. La valeur absolue usuelle étant la seule de toutes à être non archimédienne, il suffit de montrer que les valeurs absolues p-adiques sont deux à deux non équivalentes. Or si p, q sont deux nombres premiers distincts, on a $|p|_p < 1$ et $|p|_q = 1$, ce qui montre que $|\cdot|_p$ et $|\cdot|_q$ sont non équivalentes.

Soit maintenant $|\cdot|$ une valeur absolue non triviale sur $\mathbb{Q}$. Si $|\cdot|$ est non archimédienne, alors elle est bornée par 1 sur $\mathbb{Z}$ et la proposition précédente s'applique, montrant que $|\cdot|$ équivaut à une valeur absolue p-adique.

Si maintenant $|\cdot|$ est archimédienne, on va montrer en suivant [4, p.77] que $|\cdot| = |\cdot|_\infty^s$ pour un certain $s > 0$. Vu que $|-1| = 1$ et que -1 et $\mathbb{N}\backslash\{0,1\}$ engendrent $\mathbb{Q}^\times$ multiplicativement, il suffit de le montrer pour tout entier supérieur ou égal à 2. Soient donc $a, b \geq 2$. Pour tout $n \in \mathbb{N}$, on peut écrire en base a, on peut écrire $b^n = \sum_{k=0}^{m} x_k a^k$ avec $\forall k \in [\![0, m]\!], 0 \leq x_k \leq a-1$ et $x_m \neq 0$. Par l'inégalité triangulaire, $\forall x \in \mathbb{N}, |x| \leq x$ et donc

$$|b|^n \leq \sum_{k=0}^{m} x_k |a|^k \leq (m+1)(a-1)\max(1, |a|)^m.$$

Or on a $m \leq \log_a(b^n)$, d'où

$$|b|^n \leq (1 + n\log_a(b))(a-1)\max(1, |a|)^{n\log_a(b)}.$$

Donc en prenant la racine n-ième puis la limite quand n tend vers l'infini, on a $|b| \leq \max(|1|, |a|^{\log_b(a)})$. Si on avait $|a| \leq 1$, on en déduirait $|b| \leq 1$, et ce pour tout $b \geq 2$. Alors $|\cdot|$ serait non-archimédienne, ce qui est exclu. Ainsi, $|a| > 1$ et donc $|b| \leq |a|^{\log_b(a)}$. Par symétrie, on a également $|a| \leq |b|^{\log_a(b)}$, et donc en prenant $a = 2$ (par exemple), $\forall b \geq 2, |b| = |2|^{\log_2(b)} = b^{\log_2(|2|)}$, d'où $|\cdot| = |\cdot|_\infty^s$ avec $s = \log_2(|2|)$. □

On énonce maintenant une proposition qui va dans le sens contraire de la proposition 1.15, montrant que même si elles sont deux à deux non équivalentes, les valeurs absolues sur $\mathbb{Q}$ gardent entre elles une certaine forme de dépendance.

Proposition 3.3 (Formule du produit pour $\mathbb{Q}$)**.** *Pour tout $x \in \mathbb{Q}^\times$, on a*

$$\prod_{p \in \mathcal{P} \cup \{\infty\}} |x|_p = 1,$$

où $\mathcal{P}$ est l'ensemble des nombres premiers.

Démonstration. En effet, en écrivant $x = \pm \prod_{p \in \mathcal{P}} p^{v_p(x)}$, on a

$$|x|_\infty = \prod_{p \in \mathcal{P}} |p|_\infty^{v_p(x)} = \prod_{p \in \mathcal{P}} p^{v_p(x)} = \prod_{p \in \mathcal{P}} |x|_p^{-1},$$

ce qu'on voulait. □

3.2 Théorème d'Ostrowski sur $K(X)$

Soit K un corps. On a déjà vu plusieurs exemple de valeurs absolues sur $K(X)$, à savoir :

- La valeur absolue triviale.
- La valeur absolue liée au degré définie par $|\cdot|_\infty = c^{-\deg(\cdot)}$ avec $c \in]0,1[$.
- Pour chaque polynôme irréductible P de $K[X]$, la valeur absolue P-adique définie par $|\cdot|_P = c^{v_P(\cdot)}$, où $c \in]0,1[$.

Ce ne sont toutefois généralement pas les seules valeurs absolues à équivalence près sur K. Par exemple, pour $K = \mathbb{Q}$, on peut considérer n'importe quel nombre transcendant $\alpha \in \mathbb{C}$. Il y a alors un unique isomorphisme $\phi : \mathbb{Q}(X) \to \mathbb{Q}(\alpha)$ tel que $\phi(X) = \alpha$. En considérant $|\cdot|_\infty$ la valeur absolue usuelle sur $\mathbb{C}$, on obtient alors une valeur absolue $|\cdot|$ sur $\mathbb{Q}(X)$ par le transport de structure $|\cdot| = |\phi(\cdot)|_\infty$. De plus, comme $|\cdot|$ est archimédienne, elle n'est pas équivalente à une des valeurs absolues précédemment citées.

De nombreuses valeurs absolues peuvent donc apparaître sur $K(X)$, et pour simplifier le problème, on ne va donc considérer que les valeurs absolues étendant la valeur absolue triviale sur K. On dispose alors du théorème suivant (cf. [3]).

Théorème 3.4 (Théorème d'Ostrowski sur $K(X)$)**.** *Soit K un corps. Toute valeur absolue sur $K(X)$ dont la restriction à K est triviale est équivalente à une et une seule des valeurs absolues suivantes :*

- *La valeur absolue triviale.*
- *La valeur absolue provenant du degré $|\cdot|_\infty$.*
- *La valeur absolue P-adique $|\cdot|_P$ pour un polynôme irréductible unitaire $P \in K[X]$.*

Démonstration. Commençons par montrer l'unicité. La même preuve que pour $\mathbb{Q}$ montre que les $|\cdot|_P$ sont non équivalentes entre elles. De plus, $|\cdot|_\infty$ n'équivaut à aucune des $|\cdot|_P$ car pour un irréductible P, $|P|_\infty > 1$ alors que $|P|_P < 1$.

Soit $|\cdot|$ une valeur absolue sur $K(X)$ prolongeant la valeur absolue discrète. Comme $|\cdot|$ prolonge une valeur absolue ultramétrique, elle est ultramétrique. On distingue alors deux cas.

Ou bien $|X| \leq 1$, auquel cas, en appliquant la proposition 3.1 à $|\cdot|$ et l'anneau principal $K[X]$, on en déduit que $|\cdot|$ équivaut à $|\cdot|_P$ pour un certain irréductible $P \in K[X]$.

Ou bien $|X| > 1$, auquel cas tout élément de $K[\frac{1}{X}]$ est de valeur absolue plus petite que 1. On peut donc appliquer la proposition 3.1 à $|\cdot|$ et l'anneau principal $K[\frac{1}{X}]$. Il existe donc Q un irréductible de $K[\frac{1}{X}]$ tel que $|\cdot|$ équivaut à $|\cdot|_Q$. Or au vu de l'isomorphisme d'anneaux $K[X] \simeq K[\frac{1}{X}]$ (donné par $\phi : X \mapsto \frac{1}{X}$), on a $Q = P(\frac{1}{X})$ pour un certain irréductible $P \in K[X]$. Il y a alors deux possibilités. Ou bien P est associé à X, auquel cas $|\cdot|$ équivaut à $|\cdot|_{\frac{1}{X}}$, et on a déjà vu (lors des exemples suivant la définition 1.7) qu'il s'agit de $|\cdot|_\infty$. Ou bien X est premier avec P, auquel cas $P_2 = X^{\deg(P)}P(\frac{1}{X})$ est un irréductible de $K[X]$. On constate alors que $|\cdot|_Q = |\cdot|_{P_2}$, ce qui conclut. □

En particulier, comme on a vu que toute valeur absolue sur $\mathbb{F}_q$ est triviale, on en déduit alors le résultat suivant.

Corollaire 3.5. *Soit q une puissance d'un nombre premier. Toute valeur absolue sur $\mathbb{F}_q(X)$ est équivalente à une et une seule des valeurs absolues suivantes :*

- *La valeur absolue triviale.*
- *La valeur absolue provenant du degré $|\cdot|_\infty$.*
- *La valeur absolue P-adique $|\cdot|_P$ pour un polynôme irréductible unitaire $P \in \mathbb{F}_q[X]$.*

On va maintenant normaliser ces valeurs absolues (c'est à dire bien en choisir les constantes dans leur définition) afin de disposer d'une formule du produit. Soit $c \in]0,1[$, on fixe $|\cdot|_\infty = c^{-\deg(\cdot)}$ et pour tout irréductible P de $K[X]$, on fixe $|\cdot|_P = (c^{\deg(P)})^{v_P(\cdot)}$. Sous cette normalisation, on a alors la formule qui suit.

Proposition 3.6 (Formule du produit pour $K(X)$)**.** *Soit K un corps et $Q \in K(X)^\times$. On a*

$$\prod_P |Q|_P = 1,$$

où P parcourt les polynômes irréductibles unitaires de $K[X]$ et $+\infty$.

Démonstration. En effet, en écrivant $Q = a\prod_P P^{v_P(x)}$ (où le produit est sur l'ensemble des irréductibles unitaires), on a

$$|Q|_\infty = \prod_P |P|_\infty^{v_P(Q)} = \prod_P c^{-deg(P)v_P(Q)} = \prod_P |Q|_P^{-1},$$

ce qu'on voulait. □

3.3 Théorème d'Ostrowski sur un corps de nombres

Un corps de nombres est une extension finie K du corps des rationnels. Au sein d'un corps de nombres, un objet d'intérêt est son anneau des entiers qui correspond à l'ensemble des éléments de K entiers sur K. Il est usuellement noté $\mathcal{O}_K$, mais on le notera ici $\mathcal{A}_K$. En effet, il ne s'agit pas exactement de la même notion que celle définie à la page précédente (dans le cas d'un corps de nombre munit d'une valeur absolue ultramétrique, $\mathcal{O}_K$ correspond en réalité à un localisé de $\mathcal{A}_K$ par un bon idéal premier).

$\mathcal{A}_K$ est ce qu'on appelle un anneau de Dedekind. Cela signifie que chaque idéal non nul de A se factorise de façon unique en un produit d'idéaux premiers. On ne détaillera pas plus sur la question en supposant ces notions déjà connues. On peut se référer à [10] pour un exposé complet sur la question.

L'objectif de cette section est d'étudier les valeurs absolues sur K. Plusieurs d'entre-elles peuvent nous venir assez naturellement :

- La valeur absolue triviale.

- K est un sous-corps de $\mathbb{C}$, donc on dispose de la valeur absolue usuelle $|\cdot|_\infty$ qu'il suffit de restreindre à K.

- On peut généraliser le point précédent : pour chaque plongement $\sigma : K \to \mathbb{C}$, on dispose d'une valeur absolue $|\cdot|_\sigma$ donnée par $\forall x \in K, |x|_\sigma = |\sigma(x)|_\infty$. Notons au passage que si σ et $\tilde{\sigma}$ sont deux plongement conjugués (c'est à dire qu'on passe de l'un à l'autre via la conjuguaison complexe), les valeurs absolues qui en découlent sont identiques.

- Soit $\mathfrak{p}$ un idéal premier de A. Soit $x \in \mathcal{A}_K$. Comme $\mathcal{A}_K$ est un anneau de Dedekind, l'idéal xA s'écrit de façon unique $xA = \mathfrak{p}^n I$ avec $n \in \mathbb{N}$ et I un idéal de A premier avec $\mathfrak{p}$. On pose alors $v_\mathfrak{p}(x) = n$. Pour un élément $z \in K$, on écrit $z = \frac{x}{y}$ avec $x, y \in \mathcal{A}_K$, et on pose $v_\mathfrak{p}(z) = v_\mathfrak{p}(x) - v_\mathfrak{p}(y)$. Alors $v_\mathfrak{p}$ est une valuation sur K, ce qui, modulo le choix d'une constante, définit une valeur absolue $|\cdot|_\mathfrak{p}$ sur K.

Déterminons maintenant les valeurs absolues sur $\mathbb{Q}$ que ces différentes valeurs absolues prolongent.

- La valeur absolue triviale sur K prolonge la valeur absolue triviale sur $\mathbb{Q}$, et au vu de la proposition 2.27, c'est la seule dans ce cas là.

- Soit σ un plongement de K dans $\mathbb{C}$. Comme σ fixe $\mathbb{Q}$, $|\cdot|_\sigma$ prolonge la valeur absolue usuelle. En particulier, σ est archimédienne.

- Soit $\mathfrak{p}$ un idéal premier de $\mathcal{A}_K$. Alors $\mathfrak{p} \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$ et il est non nul (car il contient $N_{K/\mathbb{Q}}(x)$ pour n'importe quel $x \in \mathcal{A}_K$), ainsi on a $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ pour un certain premier p. En particulier $p\mathcal{A}_K \subset \mathfrak{p}$ et donc $v_\mathfrak{p}(p) \geq 1$. Ainsi $v_\mathfrak{p}(p) \geq 1$ et donc $|p|_\mathfrak{p} < 1$. Par le théorème d'Ostrowski sur $\mathbb{Q}$, $|\cdot|_\mathfrak{p}$ prolonge donc une valeur absolue équivalente à $|\cdot|_p$. Pour qu'elle prolonge précisément $|\cdot|_p$, il faut la normaliser de façon à ce que $|p|_\mathfrak{p} = \frac{1}{p}$. Or $|p|_\mathfrak{p} = c^{v_\mathfrak{p}(p)}$, il faut donc prendre pour constante $c = (\frac{1}{p})^{\frac{1}{v_\mathfrak{p}(p)}}$.

  On verra toutefois plus tard pour obtenir la formule du produit que ce n'est pas la normalisation la plus pertinente.

On va montrer qu'à équivalence près, les seules valeurs absolues sur K sont celles décrites ci-desssus. On suit pour cela [2] et on commence par la lemme suivant.

Lemme 3.7. *Soit $\mathfrak{p}$ un idéal premier non nul de $\mathcal{A}_K$ et $z \in K^\times$ tel que $v_\mathfrak{p}(z) \geq 0$, il existe $x, y \in \mathcal{A}_K$ avec $v_\mathfrak{p}(y) = 0$ tels que $z = \frac{x}{y}$.*

Démonstration. La décomposition en produit d'idéaux premiers permet d'écrire $z\mathcal{A}_K = \mathfrak{a}\mathfrak{b}^{-1}$ avec $\mathfrak{a}, \mathfrak{b}$ deux idéaux de $\mathcal{A}_K$ et $\mathfrak{p}$ premier avec $\mathfrak{b}$ (car $v_\mathfrak{p}(z) \geq 0$). Soit $x \in \mathfrak{a} \backslash \mathfrak{p}\mathfrak{a}$ et $\mathfrak{c} = x\mathfrak{a}^{-1}$. $\mathfrak{c}$ est un idéal de $\mathcal{A}_K$ dans la classe d'idéaux de $\mathfrak{a}^{-1}$ qui est premier avec $\mathfrak{p}$. On a alors $z\mathcal{A}_K = (\mathfrak{a}\mathfrak{c})(\mathfrak{b}\mathfrak{c})^{-1}$, alors $\mathfrak{a}\mathfrak{c} = x\mathcal{A}_K$, $\mathfrak{b}\mathfrak{c} = \frac{x}{z}\mathcal{A}_K$ et $y := \frac{x}{z}$ car $y\mathcal{A}_K$ est le produit d'idéaux de $\mathcal{A}_K$. De plus $v_\mathfrak{p}(y) = 0$ car $y\mathcal{A}_K$ est le produit de deux idéaux premier avec $\mathfrak{p}$. Comme $z = \frac{x}{y}$, on a bien la décomposition souhaitée. □

On en déduit la proposition suivante qui va nous permettre de classifier les valuations sur K.

Proposition 3.8. *Soit $|\cdot|$ une valeur absolue ultramétrique non triviale sur K. Alors $|\cdot|$ équivaut à $|\cdot|_{\mathfrak{p}}$ pour un unique idéal premier non nul $\mathfrak{p}$ de $\mathcal{A}_K$.*

Démonstration. Si un tel $\mathfrak{p}$ existe, alors il s'agit de $\{x \in \mathcal{A}_K, |x|_{\mathfrak{p}} < 1\}$, ce qui montre l'unicité.

Montrons que $A_K \subset \mathcal{O}_K$ (où $\mathcal{O}_K$ est l'anneau d'entier de K pour la valeur absolue $|\cdot|$). Soit $x \in \mathcal{A}_K$, comme x est entier sur $\mathbb{Z}$, il existe $d \in \mathbb{N}^*$ et $a_0, ...a_{d-1} \in \mathbb{Z}$ tels que $x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0 = 0$. En réécrivant $x^d = -a_{d-1}x^{d-1} - \ldots - a_1 x - a_0$, on a $|x|^d \leq \max\{|a_i||x|^i, 0 \leq i \leq d-1\} \leq |x|^{d-1}$ car pour tout $i \in [\![1, d-1]\!]$ a_i étant dans $\mathbb{Z}$ et $|\cdot|$ non archimédienne, $|a_i| \leq 1$, ainsi, $|x|^d \leq |x|^{d-1}$ et donc $|x| \leq 1$ puis $x \in \mathcal{O}_K$.

Soit maintenant $\mathfrak{p} = m_K \cap \mathcal{A}_K$, c'est un idéal premier de $\mathcal{A}_K$ comme intersection d'un idéal premier d'un suranneau avec $\mathcal{A}_K$. De plus, il est non nul car sinon, $|\cdot|$ serait triviale.

Montrons que $|\cdot|$ et $|\cdot|_{\mathfrak{p}}$ sont équivalentes. On commence par montrer que pour tout $z \in K^\times$ tel que $v_{\mathfrak{p}}(z) = 0$, $|z| = 1$. En effet, on sait qu'on peut écire $z = \frac{x}{y}$ avec $x, y \in \mathcal{A}_K$ $y \notin \mathfrak{p}$ et donc comme $v_{\mathfrak{p}}(z) = 0$, on a également $x \notin \mathfrak{p}$. Comme $x \in \mathcal{A}_K$, $|x| \leq 1$ et comme $x \notin m_K$, on a donc $|x| = 1$. On fait de même $|y| = 1$ et donc $|z| = 1$. Soit maintenant $\gamma \in \mathfrak{p}\backslash\mathfrak{p}^2$. Soit $x \in K^\times$, on a $v_{\mathfrak{p}}\left(\frac{x}{\gamma^{v_{\mathfrak{p}}(x)}}\right) = 0$, donc $\left|\frac{x}{\gamma^{v_{\mathfrak{p}}(x)}}\right| = 1$ et donc $|x| = |\gamma|^{v_{\mathfrak{p}}(x)}$, ce que l'on voulait. □

On s'intéresse maintenant au cas des valeurs absolues archimédiennes. Afin de déterminer lesquels des $|\cdot|_\sigma$ sont équivalentes on utilise la proposition suivante tirée de [9]. Soit $|\cdot|$ une valeur absolue sur $\mathbb{Q}$ et en notant toujours $|\cdot|_{\overline{\widehat{\mathbb{Q}}}}$ l'extension de $|\cdot|$ à $\overline{\widehat{\mathbb{Q}}}$, on définit pour tout plongement $\sigma : K \to \overline{\widehat{\mathbb{Q}}}$ la valeur absolue $|\cdot|_\sigma$ sur K par $|x|_\sigma = |\sigma(x)|_{\overline{\widehat{\mathbb{Q}}}}$.

Proposition 3.9. *Soit K un corps de nombre. Alors, pour $\sigma, \tau : K \to \overline{\widehat{\mathbb{Q}}}$, on a $|\cdot|_\sigma = |\cdot|_\tau$ si et seulement s'il existe $\lambda \in Aut_{\widehat{\mathbb{Q}}}\left(\overline{\widehat{\mathbb{Q}}}\right)$ tel que $\tau = \lambda \circ \sigma$.*

Démonstration. Soit $\lambda \in Aut_{\widehat{\mathbb{Q}}}\left(\overline{\widehat{\mathbb{Q}}}\right)$, comme $|\cdot|_{\overline{\widehat{\mathbb{Q}}}}$ et $|\lambda(\cdot)|_{\overline{\widehat{\mathbb{Q}}}}$ sont deux valeurs absolues prolongeant $|\cdot|_{\widehat{\mathbb{Q}}}$ à $\overline{\widehat{\mathbb{Q}}}$, elles sont identiques par 2.30. Ainsi, si $\tau = \lambda \circ \sigma$, alors $|\cdot|_\sigma = |\cdot|_\tau$.

Réciproquement, si $|\cdot|_\sigma = |\cdot|_\tau$, on considère l'isomorphisme de $\tau(K)$ sur $\sigma(K)$ donné par $\lambda := \sigma \circ \tau^{-1}$. Il s'agit d'une isométrie pour $|\cdot|_{\widehat{\mathbb{Q}}}$, en particulier, elle est uniformément continue, donc elle s'étend de façon unique aux complétés et on obtient $\widehat{\lambda} : \tau(K)\widehat{\mathbb{Q}} \to \sigma(K)\widehat{\mathbb{Q}}$ (car $\widehat{\tau(K)} = \tau(K)\widehat{\mathbb{Q}}$ par la proposition 1.22). $\widehat{\lambda}$ est un morphisme de corps par passage à la limite des lois et fixe $\widehat{\mathbb{Q}}$ car λ fixe $\mathbb{Q}$. Par extension des morphismes, on peut alors l'étendre à la clôture algébrique nous donnant un élément de $\mathrm{Aut}_{\widehat{\mathbb{Q}}}\left(\overline{\widehat{\mathbb{Q}}}\right)$. Comme $\sigma = \widehat{\lambda} \circ \tau$, on a ce qu'on souhaitait. □

Les seuls isomorphismes de $\mathbb{C}$ fixant $\mathbb{R}$ sont l'identité et la conjuguaison complexe. Ainsi, au vu de la proposition précédente, on considère que deux plongements de K dans $\mathbb{C}$ sont équivalents s'il sont égaux ou si on passe de l'un à l'autre via la conjugaison complexe et on prend Σ un ensemble de représentants des plongements de K dans $\mathbb{C}$ pour cette relation d'équivalence. On est alors en mesure de caractériser les valeurs absolues non-archimédiennes sur K.

Proposition 3.10. *Soit $|\cdot|$ une valeur absolue archimédienne sur K. Il existe un unique $\sigma \in \Sigma$ tel que $|\cdot|$ équivaille à $|\cdot|_\sigma$.*

Démonstration. L'unicité vient de la proposition et de la remarque précédente. Pour l'existence, on considère $|\cdot|$ une valeur absolue archimédienne sur K, quitte à la substituer par une valeur absolue équivalente, par le théorème d'Ostrowski sur $\mathbb{Q}$, on peut supposer que $|\cdot|$ prolonge $|\cdot|_\infty$ sur $\mathbb{Q}$. Soit $\widehat{K}$ le complété de K pour cette valeur absolue et i l'inclusion de K dans $\widehat{K}$. Comme $\mathbb{Q} \subset \overline{K}$, $\widehat{K}$ contient de façon canonique le complété de $\mathbb{Q}$ pour $|\cdot|_\infty$, c'est à dire $\mathbb{R}$. Par 1.22, on a même $\widehat{K} = i(K)\mathbb{R}$, en particulier, c'est une extension algébrique de $\mathbb{R}$ donc elle est isométrique à un sous-corps de $\mathbb{C}$ (de façon non nécessairement canonique). Ainsi, on dispose d'une isométrie σ de K dans $\mathbb{C}$ et on a donc $|\cdot| = |\cdot|_\sigma$. □

Le même raisonnement que celui qu'on vient de suivre appliqué au cas ultramétrique montre qu'une valeur $|\cdot|_\mathfrak{p}$ étendant $|\cdot|_p$ est équivalente à $|\cdot|_\sigma$ pour un certain $\sigma : K \to \widehat{\overline{\mathbb{Q}_p}}$. On aurait pu donc avoir cette approche pour caractériser les valeurs absolues ultramétrique sur un corps de nombres, à condition d'ensuite vérifier que les $|\cdot|_\sigma$ corresponde alors bien à des $|\cdot|_\mathfrak{p}$ pour un certain idéal premier.

En rassemblant les résultats des dernières propriétés, on obtient :

Théorème 3.11 (Théorème d'Ostrowski sur un corps de nombre)**.** *Toute valeur absolue sur K équivaut une unique valeur absolue parmi les suivantes :*

- *La valeur absolue triviale.*
- *Les valeurs absolues $\mathfrak{p}$-adiques avec $\mathfrak{p}$ un idéal premier non nul de $\mathcal{A}_K$.*
- *Les valeurs absolues $|\cdot|_\sigma$ pour $\sigma \in \Sigma$.*

Reste maintenant à déterminer une formule du produit. Pour cela on prend les normalisations suivantes :

- Si σ est un plongement réel de K, on prend $|\cdot|_\sigma$ tel que défini précédemment.
- Si σ est un plongement complexe non réel de K, on prend $|\cdot|_\sigma = |\sigma(\cdot)|_\infty^2$ tel que défini précédemment.
- Enfin, si $\mathfrak{p}$ est un idéal premier non nul de $\mathcal{A}_K$, on pose $|\cdot|_\mathfrak{p} = \frac{1}{N(\mathfrak{p})^{\mathfrak{v}_\mathfrak{p}(\cdot)}}$ où $N(\mathfrak{p})$ est la norme de l'idéal $\mathfrak{p}$ (cf. [4, p.206]).

On a alors :

Proposition 3.12 (Formule du produit pour un corps de nombre). *Soit $x \in K^\times$, on a*

$$\prod_v |x|_v = 1$$

où le produit parcourt toutes les valeurs absolues décrites précédemment.

Démonstration. On a

$$\prod_{\mathfrak{p}} |x|_{\mathfrak{p}} = \prod_{\mathfrak{p}} \frac{1}{N(\mathfrak{p})^{v_{\mathfrak{p}}(x)}} = \frac{1}{N\Big(\prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(x)}\Big)} = \frac{1}{N(x\mathcal{A}_K)} = \frac{1}{|N_{K/\mathbb{Q}}(x)|}.$$

De plus, on a également

$$\prod_{\sigma\in\Sigma} |x|_\sigma = \prod_{\sigma \text{ réel}} |\sigma(x)|_\infty \prod_{\text{paires de } \sigma\text{complexes}} |\sigma(x)|_\infty^2 = \left| \prod_{\sigma\in \mathrm{Hom}(K,\mathbb{C})} \sigma(x) \right| = |N_{K/\mathbb{Q}}(x)|,$$

et donc le produit total fait bien 1. □

4 Théorème de Hasse-Minkowski

4.1 Généralités d'algèbre bilinéaire

4.1.1 Formes bilinéaires

Dans cette partie, on considérera un corps K et E un K-espace vectoriel de dimension finie n.

Pour pouvoir définir et étudier les formes quadratiques, il convient d'abord de rappeler quelques notions sur les formes bilinéaires. Un exposé moins superficiel peut notamment être trouvé dans [6].

Définition 4.1 (Forme bilinéaire). *Une forme bilinéaire sur E est un application bilinéaire de $E \times E$ dans K.*

Étant donnée une base $\mathcal{E} = (e_1, ..., e_n)$ de E, et une forme bilinéaire B, on peut associer une matrice qu'on notera $\mathrm{Mat}_{\mathcal{E}}(B)$ et telle que $\mathrm{Mat}_{\mathcal{E}}(B)_{i,j} = B(e_i, e_j)$. Alors si $x, y \in E$ et si X et Y sont les vecteurs colonnes des coordonnées de x et y dans la base $\mathcal{E}$, on a $B(x, y) = {}^tX\mathrm{Mat}_{\mathcal{E}}(B)Y$. Réciproquement, si on considère une matrice $M \in \mathcal{M}_n(K)$, en gardant les notations ci dessus, on obtient une forme bilinéaire sur $\mathcal{E}$, via $B(x, y) = {}^tXMY$.

Si $\mathcal{E}$ et $\mathcal{E}'$ sont deux bases de E, on a la formule de changement de base

$$\mathrm{Mat}_{\mathcal{E}}(B) = {}^tP\mathrm{Mat}_{\mathcal{E}'}(B)P,$$

où P est la matrice de passage de $\mathcal{E}'$ à $\mathcal{E}$.

On dira que B est symétrique si sa matrice dans n'importe quelle base l'est, et ce sera le cas dans toutes les bases au vu de la formule de changement de base.

On note $K^{\times 2}$ le sous-groupe de $K^\times$ dont les éléments sont des carrés dans K. Ceci nous permet de définir la quantité suivante qui est un invariant important des formes bilinéaires.

Définition 4.2 (Discriminant d'une forme bilinéaire)**.** *Soit B un forme bilinéaire sur E, on appelle discriminant de B la quantité $disc(B) = \det(Mat_{\mathcal{E}}(B)) \in K/K^{\times 2}$ pour n'importe quelle base de $\mathcal{E}$ de B.*

En effet, via la formule de changement de base, si $\mathcal{E}$ et $\mathcal{E}'$ sont deux bases de E et P la matrice de passage de la première à la seconde, $\det(\mathrm{Mat}_{\mathcal{E}'}(B)) = \det({}^tP\mathrm{Mat}_{\mathcal{E}}(B)P) = \det(P)^2 \det(\mathrm{Mat}_{\mathcal{E}}(B)) \equiv \det(\mathrm{Mat}_{\mathcal{E}}(B)) \bmod K^{\times 2}$.

Définition 4.3 (Noyau d'une forme bilinéaire)**.** *Soit B une forme bilinéaire. On appelle noyau de B l'ensemble* $\ker(B) = \{x \in E, \forall y \in E, B(x,y) = 0\}$.

Définition 4.4 (Forme bilinéaire dégénérée)**.** *On dit qu'une forme bilinéaire B est dégénérée si* $\ker(B)$ *n'est pas réduit à* $\{0\}$.

Via la correspondance forme bilinéaire/matrice, ceci arrive si et seulement si $Mat_{\mathcal{E}}(B)$ n'est pas inversible pour une base $\mathcal{E}$ de E (et donc toute base via la formule de changement de base).

Définition 4.5 (Rang d'une forme bilinéaire)**.** *Soit B une forme bilinéaire. On appelle le rang de $Mat_{\mathcal{E}}(B)$ dans n'importe quelle base de E, et on le note $rg(B)$.*

Encore une fois, la formule de changement de base montre que cette notion est bien définie.

Proposition 4.6. *Soit B une forme bilinéaire sur E. B est non dégérée si et seulement si $x \mapsto B(x,\cdot)$ est un isomorphisme de E vers son dual E^*.*

Démonstration. En effet le noyau de cette application est exactement $\ker(B)$. □

Voici maintenant deux définitions qui vont de concert.

Définition 4.7 (Formes bilinéaires équivalentes)**.** *Soient E_1, E_2 deux K-espaces vectoriels munis respectivement des formes bilinéaires B_1 et B_2. B_1 et B_2 sont dites équivalentes s'il existe un isomorphisme $u : E_1 \to E_2$ tel que $\forall x, y \in E_1, B_1(x,y) = B_2(u(x), u(y))$. On note alors $B_1 \sim B_2$.*

Définition 4.8 (Matrices congruentes)**.** *Deux matrices $M_1, M_2 \in \mathcal{M}_n(K)$ sont dites congruentes s'il existe $P \in GL_n(K)$ tel que $M_1 = {}^tPM_2P$. On note alors $M_1 \sim M_2$.*

Il s'agit de relations d'équivalence. De plus, étant donné $\mathcal{E}_1$ une base de E_1 et $\mathcal{E}_2$ une base de E_2, B_1 équivaut à B_2 si et seulement si $\mathrm{Mat}_{\mathcal{E}_1}(B_1)$ est congruente à $\mathrm{Mat}_{\mathcal{E}_2}(B_2)$, que si $B_1 \sim B_2$ (resp. $M_1 \sim M_2$), on a $M_1 \sim M_2$ (resp. $B_1 \sim B_2$) en considérant P (resp. u) défini par la relation $\mathrm{Mat}_{\mathcal{E}_1,\mathcal{E}_2}(u) = P$.

On notera de plus que si deux formes B_1 et B_2 sont équivalentes, comme leurs matrices dans des bases données sont congruentes, elles ont même discriminant.

Finalement, on a besoin de définir la notion d'orthogonalité.

Définition 4.9 (Orthogonalité)**.** *Soit B une forme biliniéaire symétrique sur E. On dit que $x, y \in E$ sont orthogonaux pour B si $B(x, y) = 0$. On note alors $x \perp y$.*

Plus généralement :

- Une famille $(x_i)_{i\in I}$ de E est dite orthogonale si $\forall i \neq j, x_i \perp x_j$.
- Deux parties $U, V \subset E$ sont dites orthogonales si $\forall x \in U, \forall y \in V, x \perp y$.
- Si $U \subset E$, l'orthogonal de U est $U^\perp := \{x \in E, \forall y \in U, x \perp y\}$ et on pose $x^\perp = \{x\}^\perp$. On écrira parfois $U^{\perp_E}$ pour insister sur l'espace où $U^{\perp_B}$ pour insister sur la forme bilinéaire.

Proposition 4.10. *Soit B une forme bilinéaire symétrique et F un sous espace vectoriel de V, alors :*

1. *$F \subset (F^\perp)^\perp$.*
2. *Si B est non dégénérée, alors $\dim(F) + \dim(F^\perp) = \dim(E)$ et $F = (F^\perp)^\perp$.*
3. *Si B_F (la restriction de B à $F \times F$) est non dégénérée, alors $E = F \oplus F^\perp$.*
4. *Si B et B_F sont non dégénérées, $B_{F^\perp}$ est non dégénérée.*

Démonstration. Si $x \in F$ alors $\forall y \in F^\perp, x \perp y$ et donc $x \in (F^\perp)^\perp$ et donc $F \subset (F^\perp)^\perp$.

Supposons B non dégénérée, alors par la proposition 4.6, on dispose de la suite exacte

$$0 \longrightarrow F^\perp \longrightarrow E \longrightarrow F^* \longrightarrow 0$$

où la première flèche est l'inclusion et la seconde l'application $x \mapsto B(x, \cdot)|_F$, ce qui donne l'égalité en passant aux dimensions. En particulier, en l'appliquant à F et $F^\perp$, on obtient $\dim(F) = \dim((F^\perp)^\perp)$ et donc l'inclusion $F \subset (F^\perp)^\perp$ est une égalité.

Soit $x \in F \cap F^\perp$, on a $\forall y \in F, B(x, y) = 0$, donc $x \in \ker(B_F)$ puis comme B_F est non dégénérée, $x = 0$. Ainsi, $F \cap F^\perp = \{0\}$. Soit $x \in F$, $B(x, \cdot)|_F \in F^*$ donc comme B_F est non dégénérée, par la proposition 4.6, il existe $y \in U$ tel que $\forall z \in F, B(x, z) = B(y, z)$. Ainsi, $\forall z \in F, B(x - y, z) = 0$ et donc $x - y \in U^\perp$ et donc $x = y + x - y \in F \oplus F^\perp$ donc $E = F \oplus F^\perp$.

Si B et B_F sont non dégénérées, soit $x \in Ker(B_{F^\perp})$, on a $x \in F^\perp$ donc $x \perp F$ et $\forall y \in F^\perp, B(x, y) = 0$, donc $x \perp F^\perp$ donc $x \perp F \oplus F^\perp = E$ (par le troisième point) donc $x \in \ker(B)$ et comme B est non dégénérée, $x = 0$. □

Proposition 4.11. *On suppose que la caractéristique de K est différente de 2. Soit B une forme bilinéaire symétrique sur E. Alors E admet une base orthogonale pour B.*

Démonstration. Montrons le résultat par récurrence sur $n = dim(E)$. Si $n = 1$, tout vecteur non nul convient. Supposons le résultat au rang $n-1$. Il existe $x \in E$ tel que $B(x,x) \neq 0$. En effet, sinon, on aurait $\forall x, y \in E, B(x,y) = \frac{1}{2}(B(x+y,x+y) - B(x,x) - B(y,y)) = 0$. Ainsi $B_{\mathrm{Vect}(x)}$ est non dégénérée et donc $E = \mathrm{Vect}(x) + \mathrm{Vect}(x)^{\perp}$. Par hypothèse de récurrence, on peut prendre $(x_2, \ldots, x_n)$ une base orthogonale de $\mathrm{Vect}(x)^{\perp}$ et $(x, x_2, \ldots, x_n)$ est alors une base orthogonale de E. □

4.1.2 Formes quadratiques

On va majoritairement étudier la notion de forme quadratique pour des corps de caractéristique différente de 2. Toutefois, on commence par donner une définition un peu plus générale qui inclut le cas de la caractéristique 2. Étant donnée une base $\mathcal{E} = (e_1, \ldots, e_n)$ de E, pour tout $x \in E$, on notera $x_1, \ldots, x_n$ les coordonnées de x dans la base $\mathcal{E}$.

Définition 4.12 (Forme quadratique)**.** *Soit E un espace vectoriel de dimension fini sur un corps K. Une forme quadratique sur E est une fonction $q : E \to K$ telle qu'étant donnée une base $\mathcal{E}$ de E, q est un polynôme homogène de degré 2 en les coordonnées dans la base $\mathcal{E}$. Autrement dit, il existe des scalaires $a_{i,j}$ tels que $\forall x \in E, q(x) = \sum_{i<j} a_{i,j} x_i x_j$.*

Le couple (E, q) est alors qualifié de K-espace quadratique (ou tout simplement d'espace quadratique si le corps de base est clair).

Notons déjà que le fait d'être une forme quadratique ne dépend pas de la base de E considérée. En effet, si $\mathcal{E}'$ est une autre base de E, en notant resp. $x'_1, \ldots, x'_n$ les coordonnées de x dans la base $\mathcal{E}'$, en écrivant $e'_i = \sum_{j=1}^{n} m_{i,j} e_j$ pour tout $i \in [\![1, n]\!]$, on a $x_j = \sum_{i=1}^{n} m_{i,j} x'_i$ et donc

$$\begin{aligned} q(x) &= \sum_{i<j} a_{i,j} x_i x_j = \sum_{i<j} a_{i,j} x_i x_j = \sum_{i<j} a_{i,j} \Big(\sum_{k=1}^{n} m_{k,i} x'_k \Big) \Big(\sum_{l=1}^{n} m_{l,j} x'_l \Big) \\ &= \sum_{k=1}^{n} \sum_{l=1}^{n} \Big(\sum_{i<j} a_{i,j} m_{k,i} m_{l,j} \Big) x'_k x'_l. \end{aligned}$$

Ceci montre que q est bien un polynôme homogène de degré 2 en les x'_k.

On va maintenant essayer de ramener l'étude des formes quadratiques à celle des formes bilinéaires. Pour cela, on doit exclure le cas où K est de caractéristique 2 qui est un peu particulier.

Proposition 4.13. *Soient K est de caractéristique différente de 2 et E est un K-espace vectoriel de dimension finie. Une fonction $q : E \to K$ est une forme quadratique si et seulement si elle vérifie les deux points suivants :*

(i) $\forall \lambda \in K, \forall x \in E, q(\lambda x) = \lambda^2 q(x)$;

(*ii*) *L'application* $B : E \times E \to K$ *telle que* $\forall x, y \in E, B(x,y) = \frac{1}{2}(q(x+y)-q(x)-q(y))$ *est bilinéaire symétrique.*

Démonstration. Soit $\mathcal{E}$ une base de E. Si q est une forme quadratique, on a

$$q(\lambda x) = \sum_{i<j} a_{i,j}(\lambda x_i)(\lambda x_j) = \lambda^2 \sum_{i<j} a_{i,j} x_i x_j = \lambda^2 q(x)$$

et on a également

$$\begin{aligned} B(x,y) = q(x+y) - q(x) - q(y) &= \frac{1}{2}\Big(\sum_{i<j} a_{i,j}(x_i+z_i)(x_j+z_j) - \sum_{i<j} a_{i,j}x_i x_j - \sum_{i<j} a_{i,j} z_i z_j\Big) \\ &= \frac{1}{2}\sum_{i<j} a_{i,j}\big((x_i+z_i)(x_j+z_j) - x_i x_j - z_i z_j\big) \\ &= \frac{1}{2}\sum_{i<j} a_{i,j}(x_i z_j + x_j z_i) = {}^t X M Y \end{aligned}$$

avec $M \in M_n(K)$ tel que $m_{i,j} = \frac{1}{2} a_{min(i,j),max(i,j)}$ si $i \neq j$ et $m_{i,i} = a_{i,i}$. Ce qui montre que B est bilinéaire symétrique de matrice M.

Réciproquement, si (i) et (ii) sont vérifiées, on a $B(x,x) = \frac{1}{2}(q(2x) - q(x) - q(x)) = \frac{1}{2}(4q(x) - 2q(x)) = q(x)$ et donc $\forall x \in E, q(x) = {}^t X \mathrm{Mat}_{\mathcal{E}}(B) X$, et c'est donc un polynôme homogène de degré 2 en les x_i. □

Au vu de l'hypothèse de cette proposition, on se fixe maintenant, et jusqu'à la fin de cette sous-section un corps K de caractéristique différente de 2. Sauf mention du contraire, les espaces quadratiques mentionnés dans cette partie seront des K-espaces quadratiques.

On vient en réalité de montrer qu'on dispose d'une bijection entre formes quadratiques et formes bilinéaires symétriques sur E. À une forme bilinéaire symétrique B, on associe la forme quadratique définie par $q(x) = B(x,x)$ et à une forme quadratique, la forme bilinéaire symétrique définie par $B(x,y) = q(x+y, x+y) - q(x) - q(y)$, ces deux applications étant réciproques l'une de l'autre. S'il est utile de préciser d'où elle provient, on notera parfois B_q (resp. q_B) la forme bilinéaire (resp. quadratique) associée à une forme quadratique (resp. bilinéaire). Ceci nous donne en particulier accès aux définitions qui suivent.

Définition 4.14. *Soit* (E,q) *un espace quadratique. On définit les notions suivantes.*

- *Le noyau de* q *est l'ensemble* $\ker(q) := \ker(B_q)$.
- *Le rang de* q *est l'entier* $rg(q) := rg(B_q)$.
- q *est dite dégénérée si son noyau n'est pas réduit à* $\{0\}$;
- *Le discriminant de* q *est la quantité* $disc(q) := disc(B_q)$;

- *La matrice de q dans la base $\mathcal{E}$ est la matrice $Mat_{\mathcal{E}}(q) := Mat_{\mathcal{E}}(B_q)$.*

Définition 4.15. *Soient (E_1, q_1) et (E_2, q_2) des espaces quadratiques. q_1 et q_2 sont dites équivalentes si B_{q_1} et B_{q_2} le sont et on note alors $q_1 \sim q_2$.*

Proposition 4.16. *Soit (E, q) un espace quadratique. Il existe une base $\mathcal{E}$ de E et $a_1, \dots, a_n \in K$ tel que $q(x) = \sum_{i=1}^{n} a_i x_i^2$.*

Démonstration. Soit en effet $\mathcal{E} = (e_1, \dots, e_n)$ une base orthogonale de E pour B_q. En notant $a_i = B(e_i, e_i)$ pour tout $i \in [\![1, n]\!]$ et en prenant $x = \sum_{i=1}^{n} x_i e_i \in E$, on a $q(x) = B(x, x) = \sum_{i=1}^{n} \sum_{j=1}^{n} x_i x_j B(e_i, e_j) = \sum_{i=1}^{n} a_i x_i^2$. □

On introduit maintenant une notion qui est centrale dans l'étude des formes quadratiques.

Définition 4.17 (Élément représenté par une forme)**.** *Soient (E, q) un espace quadratique et $a \in K$. On dit que q représente a s'il existe $x \in E\backslash\{0\}$ tel que $q(x) = a$.*

Notons par exemple que si B_q est dégénérée, q représente 0, la réciproque étant fausse comme le montre l'exemple la forme quadratique définie sur K^2 par $q(x, y) = x^2 - y^2$.

La définition suivante est tirée de [6, p.19].

Définition 4.18. *Soit (E, q) un espace quadratique. q est dite universelle si elle représente tout élément de $K^\times$.*

Proposition 4.19. *Si une forme quadratique non dégénérée représente 0, elle est universelle.*

Démonstration. Soit $a \in K^\times$. Soit $x \in E\backslash\{0\}$ tel que $q(x) = 0$. Commme B_q est non dégénérée, il existe $y \in E$ tel que $B(x, y) \neq 0$. Pour tout $\lambda \in K$, on a $q(\lambda x + y) = \lambda^2 q(x) + 2\lambda B_q(x, y) + q(y) = 2\lambda B_q(x, y) + q(y)$, et si on prend $\lambda = \frac{a - q(y)}{2B_q(x,y)}$, on a $q(\lambda x + y) = a$. □

La condition de non-dégénérescence est nécessaire, en effet, la forme quadratique sur $\mathbb{R}^2$ définie par $q(x, y) = y^2$ représente 0 mais aucun nombre négatif.

Notons également qu'une forme quadratique peut-être universelle sans représenter 0, comme c'est le cas de $q(x) = x^2 + y^2$ sur $\mathbb{F}_3^2$.

On définit maintenant deux outils qui à partir de deux formes quadratiques permet d'en créer une troisième.

Définition 4.20. *Soient (E_1, q_1) et (E_2, q_2) des espaces quadratiques.*

- *On note $q_1 \oplus q_2$ la forme quadratique définie sur $E_1 \oplus E_2$ par $\forall (x, y) \in E_1 \times E_2, q(x, y) = q_1(x) + q_2(y)$.*
- *On note $q_1 \ominus q_2$ la forme quadratique définie sur $E_1 \oplus E_2$ par $\forall (x, y) \in E_1 \times E_2, q(x, y) = q_1(x) - q_2(y)$.*

On a alors le résultat suivant ([4, p.97]) :

Proposition 4.21. *Soient (E_1, q_1) et (E_2, q_2) des espaces quadratiques avec q_1 et q_2 non dégénérées. Alors $q_1 \ominus q_2$ représente 0 si et seulement si q_1 et q_2 représentent une valeur commune non nulle.*

Démonstration. Si q_1 et q_2 représentent $a \in K^\times$, alors il existe $x \in E_1\backslash\{0\}$ et $y \in E_2\backslash\{0\}$ tels que $q_1(x) = a$ et $q_2(x) = a$ ce qui fait que $(q_1 \ominus q_2)(x, y) = q_1(x) - q_2(y) = a - a = 0$ avec $(x, y) \neq (0, 0)$.

Récriproquement si $(q_1 \ominus q_2)(x, y) = 0$ alors $q_1(x) = q_2(y)$. Soit $a = q(x)$. Si $a \neq 0$, alors q_1 et q_2 représentent a. Sinon, comme $(x, y) \neq 0$, on a $x \neq 0$ ou $y \neq 0$. Disons $x \neq 0$. Alors q_1 réprésente 0, donc est universelle, et représente en particulier n'importe quelle valeur représentée par q_2. □

Notons que la preuve nous montre même que q_1 et q_2 représentent une valeur commune non nulle.

Soit $a \in K^\times$. En désignant par ax^2 la forme quadratique définie sur $E = K$ par $\forall x \in q(x) = ax^2$, on en déduit le corollaire suivant.

Corollaire 4.22. *Soit (E, q) un espace quadratique avec q non dégénérée. Alors q représente $a \in K^\times$ si et seulement si $q \ominus ax^2$ représente 0.*

Démonstration. Si q représente a, comme ax^2 le représente également, par la proposition précédente, $q \ominus ax^2$ représente 0.

Réciproquement, si $q \ominus ax^2$ représente 0, q et ax^2 représente une valeur commune non nulle, donc on peut choisir $x \in E$ et $y \in K^\times$ tels que $q(x) = ay^2$ puis $q(\frac{x}{y}) = a$. □

On enchaîne maintenant avec une proposition tirée de [4, p.98] qui nous permet de décomposer une forme quadratique de façon compatible avec un nombre qu'elle représente.

Proposition 4.23. *Soient (E, q) un espace quadratique de dimension n avec q non dégénérée et $a \in K^\times$. Alors q représente a si et seulement si elle équivaut à $q' \oplus ax^2$ avec q' une forme quadratique sur $\mathbb{R}^{n-1}$.*

Démonstration. Si une telle décomposition existe, q représente a. Réciproquement, si q représente a, soit $u \in E$ tel que $q(u) = a$. Alors $B_q|_{Vect(u)}$ est non dégénérée, donc par les deux derniers points de la proposition 4.10, en notant $H = Vect(u)^\perp$, on a $E = H \oplus Vect(u)$ et $B_q|_H$ est non dégénérée. On a alors $q = q|_H \oplus q|_{Vect(u)}$ avec $q|_{Vect(u)}$ équivalente à ax^2. □

On va finir par un théorème dû à Witt. Pour cela, comme dans [6, p.28], on commence par introduire une notion qui nous sera utile pour la preuve de ce théorème.

Définition 4.24 (Réflexion)**.** *Soit (E, q) un espace quadratique et $x \in E$ tel que $q(x) \neq 0$. On appelle réflexion suivant v l'application linéaire r_x caractérisée par $r_x(x) = -x$ et $r_x|_{x^\perp} = id$.*

Notons que cette définition est possible car, comme $q(x) \neq 0$, $q|_{\mathrm{Vect}(x)}$ est non dégénérée et donc $E = \mathrm{vect}(x) \oplus x^\perp$. Notons également, que $r_x = r_{\lambda x}$ pour tout $\lambda \in K^\times$ et $r_x^2 = id$. De plus, comme dans le cas euclidien, r_x est donné par la formule

$$\forall y \in E, r_x(y) = y - 2\frac{B_q(x,y)}{q(x)}x.$$

Finalement, comme dans le cas euclidien, r_x est une isométrie de l'espace quadratique au sens où elle préserve q et B_q :

$$\forall y \in E, q(r_x(y)) = q(y)$$
$$\forall y, z \in E, B_q(r_x(y), r_x(z)) = B_q(y,z).$$

Dans la preuve du théorème de Witt on aura besoin du lemme suivant :

Lemme 4.25. *Soient (E,q) un espace quadratique et $x, y \in E$ tels que $q(x) = q(y) \neq 0$. Alors il existe une reflexion r tel que $r(x) = y$ ou deux réflexions r_1 et r_2 telles que $(r_2 \circ r_1)(x) = y$.*

Démonstration. Si $q(y-x) \neq 0$, on prend $r = r_{y-x}$. On a alors

$$\begin{aligned} r(y) &= y - 2\frac{B_q(y-x,y)}{q(y-x)}(y-x) = y - 2\frac{q(y) - B_q(x,y)}{q(y)+q(x)-2B_q(x,y)}(y-x) \\ &= y - 2\frac{q(y)-B_q(x,y)}{2q(y)-2B_q(x,y)}(y-x) = y - (y-x) = x. \end{aligned}$$

Sinon, comme $q(x-y)+q(x+y) = 2q(x)+2q(y)+2B_q(x,y)-2B_q(x,y) = 4q(x) \neq 0$, on a $q(x+y) \neq 0$. On pose $r_1 = r_{x+y}$, si bien que

$$\begin{aligned} r_1(y) &= y - 2\frac{B_q(x+y,y)}{q(x+y)}(x+y) = y - 2\frac{B_q(x,y)+q(y)}{q(y)+q(x)+2B_q(x,y)}(x+y) \\ &= y - 2\frac{B_q(x,y)+q(y)}{2q(y)+2B_q(x,y)}(x+y) = y - (x+y) = -x. \end{aligned}$$

Donc en posant $r_2 = r_{x^\perp}$, on a bien $r_2(r_1(y)) = x$. □

On est maintenant en mesure d'énoncer et de prouver le théorème de Witt.

Théorème 4.26 (Théorème de Witt)**.** *Soient (E_i, q_i) des espaces quadratiques pour $i \in \{1,2,3\}$ avec les q_i non dégénérées. Si $q_1 \oplus q_3 \sim q_2 \oplus q_3$ alors $q_1 \sim q_2$.*

Démonstration. Par la proposition 4.16, il existe $a_1, ..., a_n \in K^\times$ tel que $q_3 \sim a_1x_1^2 \oplus \cdots \oplus a_nx_n^2$. On a donc $q_1 \oplus a_1x_1^2 \oplus \cdots \oplus a_nx_n^2 \sim q_2 \oplus a_1x_1^2 \oplus \cdots \oplus a_nx_n^2$. Il suffit donc de montrer le cas où $E_3 = K$ et $q_3 = ax^2$ avec $a \in K^\times$.

Soit $q = q_1 \oplus ax^2$ et $q' = q_2 \oplus ax^2$. Comme $q \sim q'$, il existe un isomorphisme ϕ de $E_1 \oplus K$ dans $E_2 \oplus K$ tel que $\forall x \in E_1 \oplus K, q'(\phi(x)) = q(x)$. Soit $v = (0,1) \in E_1 \oplus K$. On a $q'(\phi(v)) = q(v) = a = q'(v)$. Ainsi, par le lemme précédent, il existe r correspondant

à une réflexion de $(E_1 \oplus K, q')$ (ou une composée de deux telles réflexions), telle que $q'(v) = q(\phi(v))$. En posant $\psi = r \circ \phi$, on a alors $\psi(v) = v$ et $\forall x \in E_1 \oplus K, q'(\psi(x)) = q(x)$ et donc $\forall x, y \in E_1 \oplus K, B_{q'}(\psi(x), \psi(y)) = B_q(x, y)$. En particulier pour $x \in E_1 \oplus K$, on $x \perp_q v \Leftrightarrow \psi(x) \perp_{q'} v$, et comme dans $E_1 \oplus K$, $v^{\perp_q} = E_1 \times \{0\}$ et dans $E_2 \oplus K$, $v^{\perp_{q'}} = E_2 \times \{0\}$. Ainsi, ψ réalise donc un isomorphisme de $E_1 \times \{0\}$ dans $E_2 \times \{0\}$, et en notant $\tilde{\psi}$ l'application qui à $x \in E_1$ associe la projection de $\psi(x, 0)$ sur E_2, $\tilde{\psi}$ est un isomorphisme de E_1 sur E_2 tel que $\forall x \in E_1, q_2(\tilde{\psi}(x)) = q_1(x)$. En particulier, $q_1 \sim q_2$. □

4.2 Formes quadratiques sur $\mathbb{R}$

Sur $\mathbb{R}$, la classification des formes quadratiques est la suivante.

Théorème 4.27 (Classification des formes quadratiques réelles)**.** *Soit (E, q) un espace quadratique de dimension n avec q non dégénérée. Alors il existe un unique entier $p \in [\![0, n]\!]$ tel que $q \sim x_1^2 + \ldots + x_p^2 - x_{p+1}^2 - \cdots - x_n^2$.*

Démonstration. Par la proposition 4.16, q équivaut à une forme $a_1 x_1^2 + \ldots a_n x_n^2$. Quitte à permuter les a_i, il existe $p \in [\![0, n]\!]$ tel que $a_1, \ldots, a_p > 0$ et $a_{p+1}, \ldots, a_n < 0$. Les a_i tel que $i \leq p$ valent alors 1 modulo $\mathbb{R}^{\times 2} = \mathbb{R}_+^*$ et les autres -1. On a donc $q \sim x_1^2 + \ldots + x_p^2 - x_{p+1}^2 - \ldots - x_n^2$.

Pour l'unicité, si $x_1^2 + \ldots + x_p^2 - x_{p+1}^2 - \cdots - x_n^2 \sim x_1^2 + \ldots + x_q^2 - x_{q+1}^2 - \cdots - x_n^2$ avec $p > q$, alors par le théorème de Witt, $x_q^2 + \ldots + x_{p-1}^2 \sim -x_q^2 - \ldots - x_{p-1}^2$. Or la première forme représente des valeurs strictement positives et celles représentées par la seconde sont strictement négatives, ce qui est absurde. □

Ceci amène à la définition de l'invariant suivant caractérisant les formes quadratiques non dégénérées sur $\mathbb{R}$.

Définition 4.28 (Signature d'un forme quadratique réel)**.** *En reprenant les notations du théorème précédent, on appellle signature de q le couple $(p, n - p)$.*

Le théorème précédent montre la caractérisation suivante.

Corollaire 4.29. *Deux formes quadratiques réelles non dégénérées sont équivalentes si et seulement si elles ont même signature.*

4.3 Formes quadratiques sur un corps fini de caractéristique impaire

On va appliquer les résultats et méthodes développées dans la partie précédente à l'étude des formes quadratiques sur un corps fini. On suit [6, p.41].

Lemme 4.30. *Soit K un corps fini de caractéristique impaire. Soit (E, q) un espace quadratique de dimension supérieure ou égale à 2 avec q non dégénérée. Alors q est universelle.*

Démonstration. Au vu de la proposition 4.16, il suffit de traiter le cas $q = ax^2 + by^2$ avec $a, b \in K^\times$. Soit $t \in K^\times$. Comme K est un corps fini, $K^\times$ est cyclique et $K^{\times 2}$ en est un sous-groupe d'indice 2 de K. Ainsi, le cardinal de $\{ax^2, x \in K\}$ est $\frac{|K|+1}{2}$ et de même pour $\{t - by^2, x \in K\}$. Comme la somme des deux cardinaux est supérieure à $|K|$, il sont donc d'intersection non vide. Ainsi, il existe $x, y \in K$ tels que $ax^2 = t - by^2$ et donc $t = ax^2 + by^2$. Donc q représente par t. □

Lemme 4.31. *Soit (E, q) un espace quadratique de dimension n avec q non dégénérée. Alors $q \sim x_1^2 + \ldots + x_{n-1}^2 + dx_n^2$ avec d un représentant dans $K^\times$ du discriminant de q.*

Démonstration. Montrons la proposition par récurrence sur $n \in \mathbb{N}^*$. Le cas $n = 1$ est clair. Supposons le résultat au rang n et montrons le au rang $n + 1$. Soit q une forme quadratique sur un espace de dimension $n + 1$. Par le lemme précédent, q représente 1. Par la proposition 4.23, on peut donc écrire $q = x_1^2 \oplus q'$ avec q' non dégénérée sur un espace de dimension n. On a alors $\mathrm{disc}(q) = \mathrm{disc}(q')$, et en appliquant l'hypothèse de récurrence à q', on obtient le résultat escompté. □

En adjoignant la proposition précédente et l'invariance du discriminant par classe d'équivalence, on en déduit le résultat suivant.

Théorème 4.32 (Classification des formes quadratiques sur un corps fini de caractéristique impaire)**.** *Soit K un corps finis de caractéristique impaire. Deux formes quadratiques non-dégénérées sont équivalentes si et seulement si elles ont mêmes dimension et discriminant.*

En particulier, à dimension fixée, comme le discriminant est à valeur dans $K^\times / K^{\times 2} \simeq \mathbb{Z}/2\mathbb{Z}$, il y a exactement deux classes d'équivalences de formes quadratiques non dégénérées.

4.4 Formes quadratiques sur $\mathbb{Q}_p$

4.4.1 Structure de $\mathbb{Q}_p^{\times 2}$ et symbole de Legendre

Si (E, q) est un K espace quadratique et que q représente $a \in K^\times$ alors en écrivant $a = q(x)$, comme $q(\lambda x) = \lambda^2 q(x) = \lambda^2$, q représente toute la classe de a moduloe $K^{\times 2}$, l'ensemble des carrés de $K^\times$. Ainsi, on ne s'intéresse en réalité qu'aux classes modulo $K^{\times 2}$ représentées par une forme quadratique. Ceci justifie l'étude du groupe des carrés de $K^\times$.

Plus généralement, connaître les carrés de $K^\times$ permet de déterminer les éléments représentés dans le cas des espaces quadratiques de dimension 1, en effet pour $a \in K^\times$, ax^2 représente $b \in K^\times$ si et seulement si $\frac{b}{a} \in K^{\times 2}$.

On sait que le sous-groupe des carrés de $\mathbb{R}^*$ est $\mathbb{R}_+^*$. C'est un sous groupe d'indice 2 et le quotient $\mathbb{R}^*/\mathbb{R}_+^*$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Qu'en est-il dans le cas de $\mathbb{Q}_p$?

Proposition 4.33. *Soit p un nombre premier.*

- *Si p est impair, $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \simeq (\mathbb{Z}/p\mathbb{Z})^2$.*

- *Si* $p = 2$, $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \simeq (\mathbb{Z}/2\mathbb{Z})^3$.

Démonstration. On sait que tout élément $x \in \mathbb{Q}_p^\times$ s'écrit $x = up^n$ avec $u \in \mathbb{Z}_p^\times$. Donc x est un carré si et seulement si $n = v_p(x)$ est pair et u est un carré. Ainsi, en considérant l'isomorphisme $\phi : \begin{cases} \mathbb{Z}_p^\times \times \mathbb{Z} \to \mathbb{Q}_p^\times \\ (u,n) \mapsto up^n \end{cases}$, on a $\mathbb{Q}_p^{\times 2} = \phi(\mathbb{Z}_p^{\times 2} \times 2\mathbb{Z})$. Ainsi, $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \simeq (\mathbb{Z}_p^\times \times \mathbb{Z})/(\mathbb{Z}_p^{\times 2} \times 2\mathbb{Z}) \simeq \mathbb{Z}_p/\mathbb{Z}_p^{\times 2} \times \mathbb{Z}/2\mathbb{Z}$. Or, par la proposition 2.26, on sait que si p est impair, $\mathbb{Z}_p/\mathbb{Z}_p^{\times 2} \simeq (\mathbb{Z}/p\mathbb{Z}^\times)/(\mathbb{Z}/p\mathbb{Z}^{\times 2}) \simeq \mathbb{Z}/2\mathbb{Z}$ et si $p = 2$, $\mathbb{Z}_2/\mathbb{Z}_2^{\times 2} \simeq (\mathbb{Z}/8\mathbb{Z}^\times)/(\mathbb{Z}/8\mathbb{Z}^{\times 2}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$, ce qui conclut. □

Proposition 4.34. $\mathbb{Q}_p^{\times 2}$ *est un sous-groupe ouvert de* $\mathbb{Q}_p^\times$.

Démonstration. En effet, la preuve de la proposition précédente montre que

$$\mathbb{Q}_p^{\times 2} = \bigcap_{n \in \mathbb{Z}} p^{2n}\mathbb{Z}_p^{\times 2}.$$

Or, par la proposition 2.26, $\mathbb{Z}_p^{\times 2}$ est l'image réciproque des carrés modulo p (resp 2) par la projection canonique dans $\mathbb{F}_p$ (resp. $\mathbb{Z}/8\mathbb{Z}$), donc est ouvert. □

Pour mieux comprendre les éléments de $\mathbb{Z}_p^{\times 2}$, on rappelle maintenant la notion de symbole de Legendre qui permet d'étudier les carrés modulo un nombre premier impair p (et donc les carrés dans $\mathbb{Z}_p^\times$ par 2.26). Par rapport à la définition usuelle qui fait intervenir des entiers, on considère ici des entiers p-adiques, mais comme $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}_p/p\mathbb{Z}_p$, il s'agit en réalité du même outil.

Définition 4.35 (Symbole de Legendre)**.** *Soit* p *un nombre premier impair* $x \in \mathbb{Z}_p^\times$. *On définit le symbole de Legendre par*

$$\left(\frac{x}{p}\right) = \begin{cases} 1 \text{ si } x \in \mathbb{Z}/p\mathbb{Z}^{\times 2} \\ -1 \text{ sinon} \end{cases}.$$

On a $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$ dans $\mathbb{F}_p^\times$ (cf [4, p.105]) et donc

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 \text{ si } p \equiv 1[4] \\ -1 \text{ si } p \equiv 3[4] \end{cases}.$$

De plus, le symbole de Legendre est multiplicatif : $\forall x, y \in \mathbb{Z}_p^\times, \left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$. Notons que par cette dernière propriété, et en utilisant la décomposition en produit de facteurs premiers, il suffit donc de calculer $\left(\frac{q}{p}\right)$ pour tout nombre premier q afin de le connaître sur tout $\mathbb{Z}$ et donc sur tout $\mathbb{Z}_p$ car il ne dépend que de la classe modulo $\mathbb{Z}_p$.

Commençons par traiter le cas où $q = 2$, en suivant [4, p.108].

Proposition 4.36. *Soit* p *un nombre premier impair. Alors* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Démonstration. Soit K une extension de $\mathbb{F}_p$ dans laquelle X^4+1 est scindé, et soit $\alpha \in K$ une racine de K. Soit $\theta = \alpha + \frac{1}{\alpha}$. On a

$$\theta^2 = \alpha^2 + \frac{1}{\alpha^2} + 2 = \frac{\alpha^4+1}{\alpha^2} + 2 = 2,$$

donc $\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = \theta^{p-1}$.

Or par le morphisme de Frobenius, $\theta^p = \alpha^p + \frac{1}{\alpha^p}$ et comme $\alpha^8 = 1$, on a $\theta^p = \alpha + \frac{1}{\alpha} = \theta$ si $p \equiv 1, -1[8]$ et $\theta^p = \alpha^3 + \frac{1}{\alpha^3} = -\theta$ si $p \equiv 3, 5[8]$. Ainsi, $\theta^{p-1} = 1$ si $p \equiv 1, -1[8]$ et -1 sinon, d'où le résultat. □

Dans le cas où q est impair, on dispose du célèbre théorème suivant. Il s'agit d'un théorème ayant un nombre notable de preuves différentes s'appuyant sur divers aspects de la théorie des nombres. Comme on a précédemment développé la théorie des formes quadratiques, on présente ici une preuve tirée de [7] qui utilise cet outil.

Théorème 4.37 (Loi de réciprocité quadratique)**.** *Soient p, q deux nombres premiers impairs distincts. Alors,*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Démonstration. On considère l'ensemble $S = \{(x_1, \ldots, x_p) \in \mathbb{F}_q^p, x_1^2 + \cdots + x_p^2 = 1\}$. On va compter de deux façons différentes le cardinal de S.

Premièrement, $|S|$ est le nombre de façons dont la forme quadratique $f = x_1^2 + \cdots + x_p^2$ sur $\mathbb{F}_q^p$ représente 1. On considère maintenant la forme quadratique $f' = x_1x_2 + \ldots + x_{p-2}x_{p-1} + (-1)^{\frac{p-1}{2}}x_p^2$ sur $\mathbb{F}_q^p$. Alors f et f' sont non dégénérées et $\mathrm{disc}(f') = 1 = \mathrm{disc}(f)$. Au vu de la classification des formes quadratiques sur les corps finis de caractéristique impaire, f et f' sont donc équivalentes, puis $|S| = |S'|$, avec $S' = \{x \in \mathbb{F}_q^p, f'(x) = 1\}$. Soit $(x_1, ..., x_p) \in \mathbb{F}_q^p$.

Si $x_1 = x_3 = \ldots = x_{p-2} = 0$, alors $x \in S'$ si et seulement si $(-1)^{\frac{p-1}{2}}x_p^2 = 1$, ce qui donne q choix possibles pour $x_2, x_4, \ldots, x_{p-1}$ et $1 + \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)$ choix possibles pour x_p. Soit au total $q^{\frac{p-1}{2}}\left(1 + \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\right)$ possibilités.

Sinon, à $x_1, \ldots, x_{p-2}$ fixés et à x_p fixé, les $(x_2, x_4, \ldots, x_{p-1})$ tels que $x \in S$ sont les éléments de l'hyperplan affine d'équation $x_1x_2 + \ldots + x_{p-2}x_{p-1} = 1 - (-1)^{\frac{p-1}{2}}x_p^2$ et sont donc au nombre de $q^{\frac{p-1}{2}-1}$, ce qui fait au total, $(q^{\frac{p-1}{2}} - 1)qq^{\frac{p-1}{2}-1}$ choix pour x.

Finalement, on a

$$|S| = |S'| = q^{\frac{p-1}{2}}\left(q^{\frac{p-1}{2}} - \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\right) \equiv \left(\frac{q}{p}\right)\left(\left(\frac{q}{p}\right) + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right)[p].$$

Dans un second temps, on considère l'action de permutations des coordonnées de $\mathbb{Z}/p\mathbb{Z}$ sur S, c'est à dire telle que pour $k \in \mathbb{Z}/p\mathbb{Z}$, et $(x_1, \ldots, x_p) \in S$, $k.(x_1, \ldots, x_p) = (x_{k+1}, \ldots, x_{k+p})$ les indices étant considérés modulo p.

On constate alors que si $x \in S$ a toutes ses coordonnées identiques, $\mathrm{Stab}(x) = \mathbb{Z}/p\mathbb{Z}$ et sinon, $\mathrm{Stab}(x) = \{0\}$. Ainsi, la formule des classes nous donne :

$$\begin{aligned}|S| &= \sum_{a\in\mathbb{F}_q \text{ tel que } (a,\ldots,a)\in S} \mathrm{Orb}((a,\ldots,a)) + \sum_{(x_1,\cdot,c_p)\in\mathbb{F}_q^n \text{ non tous égaux}} \mathrm{Orb}((x_1,\ldots,x_p)) \\ &= \sum_{a\in\mathbb{F}_q \text{ tel que } pa^2=1} 1 + \sum_{(x_1,\ldots,x_p)\in\mathbb{F}_q^n \text{ non tous égaux}} p \\ &\equiv 1 + \left(\frac{p}{q}\right)[p].\end{aligned}$$

Ainsi, on a

$$\left(\frac{q}{p}\right)\left(\left(\frac{q}{p}\right) + (-1)^{\frac{(p-1)(q-1)}{4}}\right) \equiv 1 + \left(\frac{p}{q}\right)[p].$$

donc

$$\left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}} \equiv \left(\frac{p}{q}\right)[p]$$

et enfin

$$(-1)^{\frac{(p-1)(q-1)}{4}} \equiv \left(\frac{p}{q}\right)\left(\frac{q}{p}\right).$$

□

4.4.2 Symbole de Hilbert

La section précédente traite le cas de la représentation d'un entier par une forme quadratique de dimension 1 sur $\mathbb{Q}_p$. On va maintenant intoduire un outil qui permet d'étudier le cas de dimension 2.

Pour tout corps K, la représentation de $t \in K^\times$ par la forme quadratique $ax^2 + by^2$ équivaut à celle de 1 par la forme $\frac{a}{t}x^2 + \frac{b}{t}y^2$. Ainsi, l'étude des éléments représentés par une forme quadratique de dimension 2 se ramène à l'étude de l'équation $ax^2 + by^2 = 1$.

Soit $a \in K^\times$, pour étudier l'ensemble ci-dessus, on introduit l'ensemble $N_a = \{b \in K^\times, \exists (x, y) \in K^2, ax^2 + by^2 = 1\}$. On va étudier cet ensemble en suivant [4, p.109].

Proposition 4.38. *Soit K un corps de caractéristique différente de 2. Soit $a \in K$, alors N_a est l'ensemble des éléments de $K^\times$ représentés par la forme quadratique $x^2 - ay^2$. De plus, c'est un sous-groupe de $K^\times$ contenant $K^{\times 2}$.*

Démonstration. On pose $q = x^2 - ay^2$. Soit $b \in N_a$. Soient $u, v \in K$ tels que $au^2 + bv^2 = 1$. Si $v \neq 0$, $b = (\frac{1}{v})^2 - a(\frac{u}{v})^2$ donc b est représenté par q. Si, $v = 0$, a est un carré dans K et donc $q = x^2 - ay^2$ représente 0, donc est universelle et q représente b. Réciproquement, si q représente b, il existe $u, v \in K$ tels que $u^2 - av^2 = b$. si $u = 0$, $b + av^2 = 0$, donc $ax^2 + by^2$ est universelle et représente 1 puis $b \in N_a$. Sinon, $1 = b(\frac{1}{u})^2 + a(\frac{v}{u})^2$ et $b \in N_a$.

Si $a \in K^{\times 2}$ on a vu précédement que q était universelle et $N_a = K^\times$ est bien un groupe. Sinon, on a $1 = 1 - a \times 0^2 \in N_a$ et si $b, c \in N_a$, on peut écrire $b = x^2 - ay^2$ et $c = x'^2 - ay'^2$, d'où $bc = (x^2 - ay^2)(x'^2 - ay'^2) = (xx' + ayy')^2 - a(xy' + yx')^2 \in N_a$. Finalement, si $b \in N_a$, on écrit $b = x^2 - ay^2$, le système d'inconnues x', y'

$$\begin{cases} xx' + ayy' = 1 \\ yx' + xy' = 0 \end{cases}$$

est de déterminant $b \neq 0$ et il possède donc une solution (x', y'). Ainsi, en posant $c = x'^2 - ay'^2$, on a $c \in N_a$ et $cb = 1$, ce qui montre que b est stable par inverse. N_a est donc un sous-groupe de $K^\times$.

Enfin, comme $x^2 - ay^2$ représent tout carré, $K^{\times 2} \subset N_a$. □

Notons déjà quelques propriétés qui ressortent de la preuve précédente et de la définition de N_a.

- $\forall a, b \in K^\times, a \in N_b \Leftrightarrow b \in N_a$.
- $\forall a \in K^\times, 1 \in N_a$ et $-a \in N_a$.
- $\forall a \in K^{\times 2}, N_a = K^\times$.
- Si $a, b \in K^\times$ sont dans la même classe modulo $K^{\times 2}$, alors $N_a = N_b$.

On a vu dans la preuve précédente que si a est un carré dans K, alors $N_a = K^\times$. Mais qu'en est-il si ce n'est pas le cas ? La proposition précédente répond partiellement à cette question dans le cas des complétés de $\mathbb{Q}$.

Proposition 4.39. *Soit $K = \mathbb{R}$ ou $\mathbb{Q}_p$ pour un nombre premier p. Soit $a \in K^\times \backslash K^{\times 2}$. Alors N_a est un sous-groupe d'indice 2 de $K^\times$.*

Démonstration. Si $K = \mathbb{R}$. Soit $a < 0$. On a $N_a = \{b \in \mathbb{R}^\times, \exists (x, y) \in \mathbb{R}^2, b = x^2 - ay^2\} = \mathbb{R}_+$, car $-a > 0$.

Si $K = \mathbb{Q}_p$ avec p impair. Soit $\varepsilon \in \mathbb{Z}_p$ qui ne soit pas un carré. Par la proposition 4.33, $\{1, \varepsilon, p, \varepsilon p\}$ est un ensemble de représentants de $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$. Il suffit donc d'étudier N_ϵ, N_p et $N_{\epsilon p}$.

Si on avait $p \in N_\varepsilon$, il existerait $x, y \in \mathbb{Q}_p$ tels que $\varepsilon x^2 + py^2 = 1$ et comme $v_p(\varepsilon x^2) = 2v_p(x) \neq 1 + 2v_p(y) = v_p(py^2)$, on aurait $\min(2v_p(x), 1 + 2v_p(y)) = v_p(1) = 0$ et donc $v_p(x) = 0$ et $v_p(y) \geq 0$. Ainsi, $\frac{1}{x} \in \mathbb{Z}_p$ et $\frac{y}{x} \in p\mathbb{Z}_p$ et donc $\varepsilon = (\frac{1}{x})^2 \bmod p\mathbb{Z}_p$. Ainsi, ε serait un carré dans $\mathbb{F}_p^\times$ et donc dans $\mathbb{Q}_p^\times$, ce qui est exclu. Ainsi, $p \notin N_\varepsilon$ et par symétrie $\varepsilon \notin N_p$ et en suivant un raisonnement analogue, on obtient $\varepsilon p \notin N_\varepsilon$ et $\varepsilon \notin N_{\varepsilon p}$.

On vient de montrer que pour tout $a \in \mathbb{Q}_p^\times$ non carré, l'inclusion $N_a \subset \mathbb{Q}_p^\times$ est stricte. Comme $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ est d'ordre 4, pour vérifier que N_a est d'indice 2 dans $\mathbb{Q}_p^\times$, il suffit donc de vérifier que $\mathbb{Q}_p^{\times 2} \subset N_a$ est également stricte. Comme $-a \in N_a$, si $-a$ n'est pas un carré, on a gagné. Ceci traite donc les cas $a \in \{p, \varepsilon p\}$. Reste donc le cas $a = \varepsilon$ dont le traitement consiste à montrer que $\varepsilon \in N_\varepsilon$. La forme quadratique $\varepsilon x^2 + \varepsilon y^2$ sur $\mathbb{F}_p^2$ est non dégénérée donc représente 1 par la proposition 4.30. Il existe donc $x, y \in \mathbb{Z}_p$ tels que $\varepsilon x^2 + \varepsilon y^2 \equiv 1 \bmod p\mathbb{Z}_p$. Ainsi, $\varepsilon x^2 + \varepsilon y^2$ est un carré dans $\mathbb{Z}_p^\times$, et donc en écrivant $\varepsilon x^2 + \varepsilon y^2 = z^2$, on obtient $\varepsilon\left(\frac{x}{z}\right)^2 + \varepsilon\left(\frac{y}{z}\right)^2 = 1$, d'où, $\varepsilon \in N_\varepsilon$.

Si $K = \mathbb{Q}_2$. Un ensemble de représentant de $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ est $\{1, 3, 5, 7, 2, 6, 10, 14\}$ par la proposition 4.33.

On commence par s'intéresser à l'appartenance de b à N_a dans le cas où $a = 2\varepsilon$ et $b = 2\eta$ avec η et ϵ parcourant l'ensemble $\{1, 3, 5, 7\}$. Si $ax^2 + by^2 = 1$ alors $\min(1 + 2v_2(x), 1 + 2v_2(y)) \leq v_2(1) = 0$. Comme il ne peut y avoir égalité, par "tous les triangles sont isocèles", $v_2(x) = v_2(y)$ et $2v_2(x) + 1 < 0$ donc $z' := 2^{-2v_2(x)} \in \mathbb{Z}_2$, $x' := 2^{-v_2(x)}x \in \mathbb{Z}_2^\times$, $y' := 2^{-v_p(x)}y \in \mathbb{Z}_2^\times$ et $\varepsilon x'^2 + \eta y'^2 = 2z'^2$. Si $z' \in 2\mathbb{Z}_2$, alors

$$v_2(\varepsilon + \eta) = v_2(\varepsilon(x'^2 - 1) + \eta(y'^2 - 1) - 2z'^2) \geq 3$$

et si $z' \notin 2\mathbb{Z}_2$ on a

$$v_2(\varepsilon + \eta - 2) = v_2(\varepsilon(x'^2 - 1) + \eta(y'^2 - 1) - 2(z'^2 - 1)) \geq 3.$$

Les couples ε, η tels qu'on ait $a \in N_b$ sont donc parmi $(1,1), (1,7), (3,5), (3,7), (5,5)$ et leurs symétriques. Or $2 + 2$, $2 + 14$, $6 + 10$, $6 \times 3^2 + 14 = 4 \times 17$ et $10 \times 3^2 + 10$ sont des carrés 2-adiques, ce qui montre que pour ces couples, la forme $ax^2 + by^2$ représente bien 1. Comme chaque nombre ci dessus apparaît exactement deux fois en première position de chaque couple, pour $a = 2\varepsilon$, seuls deux classes modulo $\mathbb{Q}_2^{*2}$ parmi celles de $2, 6, 10$ et 14 sont dans N_a. Comme N_a contient également la classe de 1, on a $3 \leq [N_a : \mathbb{Q}_2^{\times 2}] \leq 6$. Comme cet indice doit diviser $[\mathbb{Q}_2^\times : \mathbb{Q}_2^{\times 2}] = 8$, c'est donc 4 puis $[\mathbb{Q}_2^\times : N_a] = 2$.

Reste maintenant à déterminer N_a pour $a \in \{3, 5, 7\}$. Comme $3 \times 4 + 5 = 17, 5 \times 4 + 5 = 25$ et $7 \times 4 + 5 = 33$ sont des carrés 2-adiques, on a $3, 5, 7 \in N_5$ et on a de plus $1 \in N_5$, ainsi $[N_5 : \mathbb{Q}_2^{\times 2}] \geq 4$ et donc $[\mathbb{Q}_2^\times : N_5] \leq 2$. Comme $7 + 2$ est un carré, $7 \in N_2$, or on a déjà vu $2, 14 \in N_2$ et on a $1 \in N_2$ et que $[\mathbb{Q}_2^\times : N_2] = 2$, donc $5 \notin N_2$ puis $2 \notin N_5$, donc $[\mathbb{Q}_2^\times : N_5] > 1$ et ainsi $[\mathbb{Q}_2^\times : N_5] = 2$.

On a vu précédemment $3 \in N_5$ et $2 \in N_3$, donc $5 \in N_3$ et $2 \notin N_3$. On a $6 + 3 \in \mathbb{Q}_2^{\times 2}$ et $14 + 3 \in \mathbb{Q}_2^{\times 2}$, d'où $6, 14 \in N_3$. Comme de plus $1 \in N_3$, N_3 contient au moins 4 classes modulo $\mathbb{Q}_2^{\times 2}$, mais pas 8 et est donc également d'indice 2 dans $\mathbb{Q}_2^\times$.

Finalement, de $7 \notin N_3$, $7 \in N_2$ et $7 \in N_5$, on a $3 \notin N_7$ et $5, 7 \in N_3$. De plus $1 \in N_7$ et comme $10 + 7$ est un carré 2-adique, $10 \in N_7$. Ainsi, N_7 est d'indice deux dans $\mathbb{Q}_2^\times$. □

La preuve a permis le calcul de N_a dans divers cas. Résumons ce qu'on a obtenu jusqu'à maintenant.

- Dans le cas de $\mathbb{R}$, on a
$$N_{-1} = \mathbb{R}_+^*.$$

- Dans le cas de $\mathbb{Q}_p$ avec p impair, en considérant une unité non carré ε, on a

$$N_\varepsilon = \mathbb{Q}_p^{\times 2} \cup \varepsilon \mathbb{Q}_p^{\times 2}.$$

- Dans le cas de $\mathbb{Q}_2$, on a

$$\begin{aligned} N_2 &= \mathbb{Q}_2^{\times 2} \cup 2\mathbb{Q}_2^{\times 2} \cup 7\mathbb{Q}_2^{\times 2} \cup 14\mathbb{Q}_2^{\times 2}, \\ N_3 &= \mathbb{Q}_2^{\times 2} \cup 5\mathbb{Q}_2^{\times 2} \cup 6\mathbb{Q}_2^{\times 2} \cup 14\mathbb{Q}_2^{\times 2}, \\ N_5 &= \mathbb{Q}_2^{\times 2} \cup 3\mathbb{Q}_2^{\times 2} \cup 5\mathbb{Q}_2^{\times 2} \cup 7\mathbb{Q}_2^{\times 2}, \\ N_7 &= \mathbb{Q}_2^{\times 2} \cup 2\mathbb{Q}_2^{\times 2} \cup 5\mathbb{Q}_2^{\times 2} \cup 10\mathbb{Q}_2^{\times 2}. \end{aligned}$$

On est maintenant en mesure de définir un nouvel outil.

Définition 4.40 (Symbole de Hilbert)**.** *Soit $K = \mathbb{R}$ où $\mathbb{Q}_p$. Soient $a, b \in K^\times$. On définit le symbole de Hilbert par $(a,b)_K = 1$ si $a \in N_b$ et $(a,b)_K = -1$ sinon.*

On notera également le symbole de Hilbert par $(\cdot,\cdot)_\infty$ quand $K = \mathbb{R}$ et $(\cdot,\cdot)_p$ quand $K = \mathbb{Q}_p$.

Comme $a \in N_b \Leftrightarrow b \in N_a$, le symbole de Hilbert est symétrique. De plus, le fait d'avoir établi précédent que N_b est un sous-groupe d'indice 2 de K montre qu'il est bimultiplicatif : $\forall x, y, z \in K^\times, (xy, z)_K = (x,z)_K (y,z)_K$. Si $x \in K^{\times 2}$, $\forall y \in K^\times (x,y)_K = 1$. Enfin, le symbole de Hilbert ne dépend que des classe modulo $K^{\times 2}$ des éléments considérés.

En particulier, à partir de $(-1,-1)_\infty = -1$, on le connaît totalement sur $\mathbb{R}$ et pour le connaître sur $\mathbb{Q}_p$, il suffit de déterminer pour $\varepsilon, \eta \in \mathbb{Z}_p^\times$ les valeurs de $(\varepsilon,\eta)_p$, $(\varepsilon,p)_p$ et $(p,p)_p$. Ceux-ci nous sont donnés par la proposition suivante.

Proposition 4.41. *Soit p un nombre premier impair, et $\varepsilon, \eta \in \mathbb{Z}_p^\times$, on a*

$$\begin{aligned} (\varepsilon,\eta)_p &= 1, \\ (\varepsilon,p)_p &= \left(\frac{\varepsilon}{p}\right), \\ (p,p)_p &= \left(\frac{-1}{p}\right). \end{aligned}$$

Soient $\varepsilon, \eta \in \mathbb{Z}_2^\times$. En notant $\tilde{\varepsilon}$ et $\tilde{\eta}$ leur projection dans $\mathbb{Z}/8\mathbb{Z}$, on a

$$\begin{aligned} (\varepsilon,\eta)_2 &= (-1)^{\frac{(\tilde{\varepsilon}-1)(\tilde{\eta}-1)}{4}}, \\ (\varepsilon,2)_2 &= (-1)^{\frac{\tilde{\varepsilon}^2-1}{8}}, \\ (2,2)_2 &= 1. \end{aligned}$$

Démonstration. Soit p un nombre premier impair et $\varepsilon, \eta \in \mathbb{Z}_p^\times$. Si ε est un carré $(\varepsilon, \eta)_p = 1$ et $(\varepsilon, p)_p = 1$. Si ε n'est pas un carré, $N_\varepsilon = \mathbb{Q}_p^{\times 2} \cup \varepsilon \mathbb{Q}_p^{\times 2}$, avec $\mathbb{Q}_p^{\times 2}$ contenant les carrés de $\mathbb{Z}_p^\times$ et $\varepsilon \mathbb{Q}_p^{\times 2}$ contenant les élément non carrés de $\mathbb{Z}_p^\times$, donc $\eta \in N_\varepsilon$ et $(\varepsilon, \eta)_p = 1$, de plus, p n'est dans aucune de ces classes, donc $(\varepsilon, \eta)_p = -1$. On a donc montré les deux premières formules. La troisième se déduit de la deuxième en utilisant le fait que $-p \in N_p$ et donc $(p,p)_p = (p,-p)_p(p,-1)_p = (p,-1)_p = \left(\dfrac{-1}{p}\right)$.

On traite maintenant les formules pour $p = 2$. Comme $2 \in N_2$, on a la dernière formule. Pour la deuxième, $\varepsilon \in N_2$ si et seulement s'il est dans la classe de 1 ou 7 modulo $\mathbb{Q}_2^{2\times}$, c'est à dire si ε vaut 1 ou 7 modulo $8\mathbb{Z}_2$. Comme $(-1)^{\frac{\tilde{\varepsilon}^2-1}{8}}$ vaut 1 si $\tilde{\varepsilon} \in \{1,7\}$ et -1 si $\tilde{\varepsilon} \in \{3,5\}$, la deuxième formule est vraie. Finalement, pour la première formule, au vu des classes modulo $\mathbb{Q}^{\times 2}$ contenues dans N_1, N_3, N_5 et N_7, $\varepsilon \in N_\eta$ si et seulement si l'un des deux est 1 ou 5 modulo $8\mathbb{Z}_2$, et c'est bien les seuls cas où la formule donnée pour $(\varepsilon, \eta)_2$ donne 1. □

Le théorème qui suit est une réécriture de la loi de réciprocité quadratique à l'aide du symbole de Hilbert.

Théorème 4.42 (Loi de réciprocité de Hilbert)**.** *Soient $a, b \in \mathbb{Q}^\times$. On a*

$$\prod_p (a,b)_p = 1,$$

où p parcourt les nombres premiers et ∞.

Démonstration. Par bimultiplicativité et symétrie du symbole de hilbert, en décomposant a, b en produit de facteurs premiers, il suffit de le montrer dans les cas où $(a,b) \in \{(-1,-1),(-1,q),(q,q')\}$ avec q, q' des nombres premiers.

Comme -1 est une unité p-adique pour tout nombre premier p, $(-1,p)_p = 1$ si p est impair et donc

$$\prod_p (-1,-1)_p = (-1,-1)_\infty (-1,-1)_2 = (-1)(-1) = 1.$$

Comme q est une unité p-adique pour tout nombre premier $p \neq q$, pour tout $p \neq q$ impair, $(-1,q)_p = 1$. Donc si q est impair,

$$\prod_p (-1,q)_p = (-1,q)_\infty (-1,q)_2 (-1,q)_q = (-1)^{\frac{(-1-1)(q-1)}{4}} \left(\frac{-1}{q}\right) = (-1)^{\frac{-(q-1)}{2}} (-1)^{\frac{q-1}{2}} = 1,$$

et si $q = 2$,

$$\prod_p (-1,2)_p = (-1,2)_\infty (-1,2)_2 = (-1)^{\frac{(-1)^2-1}{8}} = 1.$$

Si $q = q'$, comme pour tout p (y compris l'infini), $(q,q)_p = (-1,q)_p$ et on a

$$\prod_p (q,q)_p = \prod_p (-1,q)_p = 1.$$

Si $q \neq q'$ avec $q' = 2$, alors comme 2 et q sont des unités p-adiques pour p distinct de 2 et q, on a $(q,2)_p = 1$ pour tout premier impair différent de q. Ainsi,

$$\prod_p (q,2)_p = (q,2)_2 (q,2)_q = (-1)^{\frac{q^2-1}{8}} \left(\frac{2}{q}\right) = 1.$$

Finalement, si $q \neq q'$ sont impairs, par la loi de réciprocité quadratique, on a

$$\prod_p (q,q')_p = (q,q')_2 (q,q')_q (q,q')_q = (-1)^{\frac{(q-1)(q'-1)}{4}} \left(\frac{q'}{q}\right)\left(\frac{q}{q'}\right) = 1.$$

□

On va avoir besoin du théorème suivant, dû à Dirichlet. On peut trouver sa preuve dans [4, p.254].

Théorème 4.43 (Théorème de la progression arithmétique)**.** *Soient $a, b \in \mathbb{Z}$ premiers entre eux. Il existe une infinité de nombres premiers p tels que $p \equiv a[b]$.*

La proposition suivante est tirée de [11, p.24].

Proposition 4.44. *Soient $(a_i)_{i\in I}$ une famille finie d'éléments de $\mathbb{Q}^\times$ et $(\varepsilon_{i,v})_{i\in I, v\in V}$ une famille d'éléments de $\{1,-1\}$ où V désigne l'ensemble des nombres premiers auquel on a adjoint $+\infty$. Alors il existe $x \in \mathbb{Q}^\times$ tel que $\forall i \in I, \forall v \in V, (x,a_i)_v = \varepsilon_{i,v}$ si et seulement si les trois conditions suivantes sont remplies.*

(i) Seul un nombre fini de $\varepsilon_{i,v}$ valent -1 ;

(ii) $\forall i \in I, \prod_{v\in V} \varepsilon_{i,v} = 1$;

(iii) Pour tout $v \in V$, il existe $x_v \in \mathbb{Q}_v$ tel que $\forall i \in I, (x_v, a_i)_v = \varepsilon_{i,v}$.

Démonstration. Le sens direct est donné par la loi de réciprocité de Hilbert. Montrons le sens réciproque. Soit deux familles (a_i) et $(\varepsilon_{i,v})$ vérifiant les conditions ci-dessus. Quitte à multiplier les a_i par les carrés de leurs dénominateurs (ce qui ne change pas les valeurs prises par les symboles de Hilbert), on peut les supposer entiers. Soient S le sous ensemble de V contenant $2, \infty$ et les diviseurs premiers des a_i. Soit $T = \{v \in V, \exists i \in I, \varepsilon_{i,v} = -1\}$. On distingue deux cas.

Si $S \cap T = \emptyset$, on pose $a = \prod_{v\in T\setminus\{\infty\}} v$ et $b = 8 \prod_{v\in V\setminus\{2,\infty\}} v$. Alors a et b sont premiers entre eux, donc on peut prendre un nombre premier $p \notin S \cup T$ tel que $p \equiv a[b]$. Montrons que $x = ap$ convient.

Si $v \in S$, alors $v \notin T$ et donc $\varepsilon_{i,v} = 1$. Soit $i \in I$, il s'agit donc de montrer que $(x, a_{i,v})_v = 1$ pour tout v. Si $v = \infty$, cela découle de $x > 0$. Si v est impair (resp. $v = 2$), $x \equiv a^2[p]$ (reps. $x \equiv a^2[8]$) donc x est un carré de $\mathbb{Q}_v^\times$ et $(x, a_{i,v})_v = 1$.

Si $v \notin S$, a_i est une unité v-adique, donc par la proposition 4.41,

$$\forall y \in \mathbb{Q}_v, (y, a_{i,v})_v = \left(\frac{a_i}{v}\right)^{v_v(y)}.$$

Dans le cas où de plus $v \notin T \cap \{p\}$, x est une unité v-adique, donc $v_v(x) = 0$ et $(x, a_{i,v})_v = 1$ comme voulu.

Dans le cas où de plus $v \in T$, $v_v(x) = 1$ et on sait qu'il existe $x_v \in \mathbb{Q}_v^\times$ tel que $(x_v, a_i) = \varepsilon_{v,i}$ pour tout $i \in I$. Comme $v \in T$, l'un des $\varepsilon_{v,i}$ vaut -1, et donc en prenant $y = x_v$ dans la formule précédente, $v_v(x_v) \equiv 1[2]$. On a alors

$$(x, a_{i,v})_v = \left(\frac{a_i}{v}\right) = (x_v, a_{i,v})_v = \varepsilon_{v,i}.$$

Finalement, le cas $v = p$ se déduit des autres cas et de la loi de réciprocité de Hilbert. En effet,

$$\forall i \in I, (x, a_i)_p = \prod_{v' \in V \setminus \{p\}} (x, a_i)_{v'} = \prod_{v' \in V \setminus \{p\}} \varepsilon_{i,v'} = \varepsilon_{i,p}.$$

Si maintenant $S \cap T$ est non vide, pour tout $v \in S$, on prend x_v tel que $\forall i \in I, (x_v, a_i)_v = \varepsilon_{i,v}$. Par la proposition 4.34, pour tout $v \in S$, $x_v \mathbb{Q}_v^{\times 2}$ est un ouvert de $\mathbb{Q}_v^\times$. Par la proposition 1.15, on peut alors prendre $x' \in \mathbb{Q}^\times$ tel que $x' \in \bigcap_{v \in S} x_v \mathbb{Q}_v^{\times 2}$. Soit $v \in S$, comme $x' \in x_v \mathbb{Q}_v^{\times 2}$, $\forall i \in I, (x', a_i)_v = (x_v, a_i)_v = \varepsilon_{i,v}$. Pour tout $i \in I$ et $v \in V$, on pose alors $\varepsilon'_{i,v} = \varepsilon_{i,v}(x', a_i)_v$. Les familles $\varepsilon'_{i,v}$ et $(a_i)_i$ vérifient alors $(i), (ii)$ et (iii) et de plus, si $v \in S$, $\forall i \in I, \varepsilon'_{i,v} = 1$. On peut alors appliquer la partie précédente et trouver $y \in \mathbb{Q}^\times$ tel que $\forall v \in V, \forall i \in I, (y, a_i)_v = \varepsilon'_{i,v}$. En prenant $x = x'y$, on a alors $\forall v \in V \forall i \in I, (x, a_i)_v = \varepsilon_{i,v}$. □

4.4.3 Symbole de Hasse

On va s'employer à définir le symbole de Hasse d'une forme quadratique qui se révélera être invariant au sein d'une classe de similitude. Pour cela, on en donne une première définition qui dépend d'un choix de base orthogonale et notre objectif sera de montrer par la suite que le symbole ne dépend pas de la base.

Définition 4.45 (Symbole de Hasse dans une certaine base)**.** *Soit $K = \mathbb{R}$ ou $\mathbb{Q}_p$. Soit (E, q) un K-espace quadratique avec q non dégénérée. Soit $\mathcal{E} = (e_1, \ldots, e_n)$ une base de $\mathcal{E}$ dans laquelle $Mat_{\mathcal{E}}(q)$ est diagonale. Notons $a_1, \ldots, a_n$ les coefficients diagonaux de cette dernière. On définit la symbole de Hasse de q dans la base $\mathcal{E}$ par*

$$c_{K,\mathcal{B}}(q) = \prod_{1 \leq i < j \leq n} (a_i, a_j)_K.$$

Notons que comme $a_i = q(e_i)$, on a $c_{K,\mathcal{B}}(q) = \prod_{1 \leq i < j \leq n} (q(x_i), q(x_j))_K$.

Les lemmes qui suivent sont tirés de [6, p.61] et ont pour objectif de montrer que $c_{K,\mathcal{B}}(q)$ ne dépend en réalité pas de la base $\mathcal{B}$ telle que $\mathrm{Mat}_{\mathcal{B}}(q)$ est diagonale.

Lemme 4.46. *Soit (E, q) un espace quadratique avec q non dégénérée. Soit $\mathcal{E} = (e_1, \dots, e_n)$ et $\mathcal{E}' = (e'_1, \dots, e'_n)$ deux bases orthogonale de E pour B_q. Alors il existe $m \in \mathbb{N}$ et des bases orthogonales $\mathcal{E}_i = (e_{i,1}, \dots, e_{i,n})$ de E pour B_q telles que*

- *$\mathcal{E}_1 = \mathcal{E}$ et $\mathcal{E}_m = \mathcal{E}'$;*
- *pour tout $1 \leq i \leq m-1$, les bases $\mathcal{E}_i$ et $\mathcal{E}_{i+1}$ diffèrent d'au plus deux vecteurs.*

Démonstration. Notons d'abord que lors de la preuve on peut considérer des bases non ordonnées . En effet, une permutation de vecteurs de la base se décompose en produit de transpositions et une transpotions ne déplace que deux vecteurs.

Montrons le résultat par récurrence sur la dimension n de E. Celui-ci est trivial si $n = 1$ ou $n = 2$. Soit $n \geq 3$, supposons le résultat au rang $n-1$ pour et montrons le au rang n. Comme $(e_1, \dots, e_n)$ est une base de E, e'_1 est une combinaison linéaire des e_i. Quitte à permuter les vecteurs de $\mathcal{E}$, on peut supposer

$$e'_1 = \sum_{i=1}^{s} a_i e_i$$

avec $s \geq 1$ et $a_1, \dots, a_s$ non nuls. On va montrer qu'on peut se ramener au cas où $s = 1$. Si $s > 1$, il existe alors $1 \leq j < k \leq s$ tel que $q(a_j e_j + a_k e_k) \neq 0$. En effet, si $s = 2$, $q(a_1 e_1 + a_2 e_2) = q(e'_1) \neq 0$ car q est non dégénérée et si $s \geq 3$, et si $s \not\geq 3$, alors

$$\begin{cases} 0 = q(a_1 e_1 + a_2 e_2) = a_1^2 q(e_1) + a_2^2 q(e_2) \\ 0 = q(a_1 e_1 + a_3 e_3) = a_1^2 q(e_1) + a_3^2 q(e_3) \\ 0 = q(a_2 e_2 + a_3 e_3) = a_2^2 q(e_2) + a_3^2 q(e_3) \end{cases}$$

donne $q(e_1) = q(e_2) = q(e_3) = 0$ ce qui est impossible comme q est non dégénérée. Quitte à permuter les vecteurs de la base, on peut donc supposer $q(a_1 e_1 + a_2 e_2) \neq 0$. Ainsi, $B_q|_{\mathrm{Vect}(a_1 e_1 + a_2 e_2)}$ est non dégénérée et en notant S son orthogonal dans $\mathrm{Vect}(e_1, e_2)$, on a donc $\mathrm{Vect}(a_1 e_1 + a_2 e_2) \oplus S = \mathrm{Vect}(e_1, e_2)$. En écrivant $s = \mathrm{Vect}(x)$ pour un certain x, $(a_1 e_1 + a_2 e_2, e_3, \dots, e_n, x)$ est une base orthogonale de E dont deux vecteurs seulement diffèrent des vecteurs de $\mathcal{E}$ pour B_q et e'_1 est alors combinaison linéaire des $s-1$ premiers vecteurs de cette base.

On réitère alors le processus ci dessus jusqu'à obtenir une base orthogonale $\mathcal{F} = (f_1, \dots, f_n)$ de E telle que $e'_1 \in Vect(f_1)$. Un unique changement de vecteur nous donne alors la base $\mathcal{F}' = (e'_1, f_2 \dots, f_n)$ qui est encore orthogonale pour B_q car $e'_1 \in Vect(f_1)$. En appliquant l'hypothèse de récurrence à $e_1'^{\perp}$ dont $(f_2, \dots, f_n)$ et $(e'_2, \dots, e'_n)$ sont des bases, on peut alors passer de $\mathcal{F}'$ à $\mathcal{E}'$, ce qui conclut. □

Lemme 4.47. *Soit $K = \mathbb{R}$ ou $\mathbb{Q}_p$ et soit (E, q) un K-espace quadratique de dimension 2 avec q non dégénérée. Soit $\mathcal{E}$ une base orthogonale de E pour B_q. Soit $z \in K^\times$. Alors q représente z si et seulement si $(z, -disc(q))_K = c_{K,\mathcal{E}}(q)$.*

Démonstration. En écrivant $\mathrm{Mat}_{\mathcal{E}}(q) = Diag(a_1, a_2)$, on a $q \sim a_1 x^2 + a_2 y^2$. Ainsi, q réprésente z si et seulement si $a_1 x^2 + a_2 y^2$ le représente, si et seulement s'il existe $x, y \in K$

tels que $\frac{a_1}{z}x^2 + \frac{a_2}{z}y^2 = 1$ si et seulement si $(\frac{a}{z}, \frac{b}{z})_K = 1$. Or on a

$$\begin{aligned}\left(\frac{a}{z}, \frac{b}{z}\right)_K &= (az, bz)_K = (a, b)_K(a, z)_K(z, b)_K(z, z)_K \\ &= c_{K,\mathcal{E}}(a, z)_K(z, b)_K(z, -1)_K = c_{K,\mathcal{E}}(z, -ab)_K \\ &= c_{K,\mathcal{E}}(q)(z, -\mathrm{disc}(q))_K,\end{aligned}$$

et donc q représente z si et seulement si $(z, -\mathrm{disc}(q))_K = c_{K,\mathcal{E}}(q)$. □

Cette formule montre en particulier qu'en dimension 2, $c_{K,\mathcal{E}}(q)$ ne dépend pas de $\mathcal{E}$ car ni le fait que $z \in K^\times$ soit ou non représénté, ni $\mathrm{disc}(q)$ n'en dépendent.

Proposition 4.48. *Soit $K = \mathbb{R}$ ou $\mathbb{Q}_p$ et soit (E, q) un K-espace quadratique avec q non dégénérée. Soient $\mathcal{E}$ et $\mathcal{E}'$ deux bases orthogonales de E pour B_q. Alors $c_{K,\mathcal{E}}(q) = c_{K,\mathcal{E}'}$.*

Démonstration. Soit $(\mathcal{E}_i)_{1\leq i\leq m}$ comme dans le lemme 4.46. Soit $1 \leq i \leq m-1$, montrons que $c_{K,\mathcal{E}_i}(q) = c_{K,\mathcal{E}_{i+1}}(q)$. En écrivant $\mathcal{E}_i = (x_1, \ldots, x_n)$ et $\mathcal{E}_i = (y_1, \ldots, y_n)$, on sait que seules deux des coordonnées diffèrent. Par symétrie du symbole de Hilbert, $c_{K,(y_1,\ldots,y_n)}(q) = c_{K,(y_{\sigma(1)},\ldots,y_{\sigma(n)})}(q)$ pour tout $\sigma \in S_n$, et on peut donc supposer que $\forall i \leq n-2, x_i = y_i$. Notons $F = Vect(x_1, \ldots, x_{n-1})$, de telle façon que $Vect(x_{n-1}, x_n) = F^\perp = Vect(y_{n-1}, y_n)$. En utilisant la remarque suivant le lemme précédent (qui donne le cas $n = 2$ de cette proposition), on a alors

$$\begin{aligned}c_{K,\mathcal{E}_{i+1}}(q) =& \prod_{1\leq j<k<n} (q(y_j), q(y_k))_K \\ =& \left(\prod_{1\leq j<k<n-2} (q(x_j), q(x_k))_K\right)\left(\prod_{1\leq j<n-1} (q(x_j), q(y_{n-1})q(y_n)))_K\right)(q(y_{n-1}), q(y_n))_K \\ =& \left(\prod_{1\leq j<k<n-2} (q(x_j), q(x_k))_K\right)\left(\prod_{1\leq j<n-1} (q(x_j), \mathrm{disc}(q|_{F^\perp}))_K\right)c_{K,(y_n,y_{n-1})}(q|_{F^\perp}) \\ =& \left(\prod_{1\leq j<k<n-2} (q(x_j), q(x_k))_K\right)\left(\prod_{1\leq j<n-1} (q(x_j), \mathrm{disc}(q|_{F^\perp}))_K\right)c_{K,(x_n,x_{n-1})}(q|_{F^\perp}) \\ =& \left(\prod_{1\leq j<k<n-2} (q(x_j), q(x_k))_K\right)\left(\prod_{1\leq j<n-1} (q(x_j), q(x_{n-1})q(x_n))_K\right)(q(y_{n-1}), q(y_n))_K \\ =& \prod_{1\leq j<k<n} (q(x_j), q(x_k))_K \\ =& c_{K,\mathcal{E}_i}(q).\end{aligned}$$

La suite $(c_{K,\mathcal{E}_i}(q))_{1\leq i\leq m}$ est donc constante, puis $c_{K,\mathcal{E}}(q) = c_{K,\mathcal{E}_1}(q) = c_{K,\mathcal{E}_m}(q) = c_{K,\mathcal{E}'}(q)$. □

La proposition précédente permet la définition qui suit.

Définition 4.49 (Symbole de Hasse)**.** *Soit $K = \mathbb{R}$ ou $\mathbb{Q}_p$. Soit (E, q) un K-espace quadratique avec q non dégénérée. On appelle symbole de Hasse de q noté $c_K(q)$ la quantité $c_{K,\mathcal{E}}(q)$ pour n'importe quelle base orthogonale $\mathcal{E}$ de E pour B_q.*

On notera parfois $c_p(q)$ si $K = \mathbb{Q}_p$.

Proposition 4.50. *Si q et q' sont deux formes quadatriques non dégénérées équivalentes, elles ont même symbole de Hasse.*

Démonstration. Soit (E, q) et (E', q') des espaces quadratique avec q, q' non dégénérées et $q \sim q'$. On considère un isomorphime $u : E \to E'$ compatible avec q et q'. Soit $\mathcal{E}$ une base orthogonale de (E, B_q), alors $u(\mathcal{E})$ est une base orthogonale de $(E', B_{q'})$ et $\mathrm{Mat}_{\mathcal{E}}(q) = \mathrm{Mat}_{u(\mathcal{E})}(q')$. On a donc $c_{K,\mathcal{E}}(q) = c_{K,u(\mathcal{E})}(q')$, ce qu'on voulait. □

4.4.4 Classification des formes quadratiques sur $\mathbb{Q}_p$

Les outils précédemment développés nous permettent d'aboutir au théorème suivant (cf. [4, p.120]). Dans ce qui suit on se permettra de désigner par $\mathrm{disc}(q)$ n'importe quel représentant de $\mathrm{disc}(q)$ dans $K^\times$.

Théorème 4.51. *Soit $K = \mathbb{R}$ ou $\mathbb{Q}_p$. Soit (E, q) un K-espace quadratique de dimension n avec q non dégénérée. Pour que q représente 0, il faut et il suffit qu'une des conditions suivantes soit réalisée :*

- *$n = 2$ et $-disc(q) \in K^{\times 2}$;*
- *$n = 3$ et $(-1, -d(q))_K = c_K(q)$;*
- *$n = 4$ et ($disc(q) \notin K^\times$ ou $(-1,-1)_K = c_K(q)$) ;*
- *$n \geq 5$ et si $K = \mathbb{R}$, les coordonnées de la signature de q sont strictement positives.*

Démonstration. La représentation de 0 étant un invariant d'une classe d'équivalente, on peut remplacer q par $\sum_{i=1}^{n} a_i x_i^2$ avec les $a_i \in K^\times$. On traite alors les dimensions une par une.

Si $\underline{n = 1}$, comme q est non dégénérée, elle ne représente pas 0.

Si $\underline{n = 2}$ et q représente 0, alors il existe $x_1, x_2 \in K^\times$ non tous deux nuls tels que $a_1x_1^2 + a_2x_2^2 = 0$. Supposons par exemple x_2 non nul, $-\frac{a_1}{a_2} = (\frac{x_1}{x_2})^2$ et donc $-\mathrm{disc}(q) = -\frac{a_1}{a_2}a_2^2 \in K^{\times 2}$. Réciproquement si $-a_1a_2 = -\mathrm{disc}(q)$ est un carré alors on peut écrire $-a_1a_2 = x^2$ et donc $a_1 + a_2(\frac{x}{a_2})^2 = 0$, ce qui montre que q représente 0.

Si $\underline{n = 3}$, alors par le corollaire 4.22, $a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ représente 0 si et seulement si $a_1x_1^2 + a_2x_2^2$ représente $-a_3$ si et seulement si $(-a_3, -\mathrm{disc}(a_1x_1^2 + a_2x_2^2))_K = c_{K,\mathcal{E}}(a_1x_1^2 +$

$a_1x_2^2$) par le lemme 4.47. Or

$$\begin{aligned}(-a_3,-a_1a_2)_K=(a_1,a_2)_K &\Leftrightarrow (-1,-a_1a_2)_K(a_3,-1)_K(a_3,a_1)_K(a_3,a_2)_K=(a_1,a_2)_K\\ &\Leftrightarrow (-1,-a_1a_2a_3)_K=(a_1,a_2)_K(a_3,a_1)_K(a_3,a_2)_K\\ &\Leftrightarrow (-1,-\mathrm{disc}(q))_K=c_K(q).\end{aligned}$$

Si $\underline{n=4}$, par la proposition 4.21 alors $a_1x_1^2+a_2x_2^2+a_3x_3^2+a_4x_4^2$ représente 0 si et seulement si $a_1x_1^2+a_2x_2^2$ et $-a_3x_3^2-a_4x_4^2$ représentent un même vecteur $x\in K^\times$. Ceci équivaut par le lemme 4.47 à l'existence d'un $x\in K^\times$ tel que $(x,-a_1a_2)_K=(a_1,a_2)_K$ et $(x,-a_3a_4)_K=(-a_3,-a_4)_K$. Soient

$$\begin{aligned}E=&\{x\in K^\times,(x,-a_1a_2)_K=(a_1,a_2)_K\}\\ E'=&\{x\in K^\times,(x,-a_3a_4)_K=(a_3,a_4)_K\}.\end{aligned}$$

Alors q représente donc 0 si et seulement si $E\cap E'$ est non vide.

Comme $(a_1,-a_1a_2)_K=(a_1,-a_1)_K(a_1,a_2)_K=(a_1,a_2)_K$, on a $a_1\in E$, et de même $a_2\in E'$. Ainsi, E et E' sont non vides. Par la proposition 4.39, on en déduit que E et E' contiennent chacun soit toutes les classes de $K^\times/K^{\times2}$, soit la moitié d'entre elles. $E\cap E'$ ne peut donc être vide que dans le cas où E contient la moitié des classes et E' l'autre moitié. Dans ce cas là $1\in E$ et $1\notin E'$ (ou vice-versa), mais alors $1=(1,-a_1a_2)_K=(a_1,a_2)_K$ et $1\neq(1,-a_3a_4)_K=(a_3,a_4)_K$ et donc $(a_1,a_2)_K=-(-a_3,-a_4)_K$ (et de même dans l'autre cas). Sous cette condition,

$$\begin{aligned}E\cap E'=\emptyset &\Leftrightarrow \forall x\in K^\times,(x,-a_1a_2)_K=(x,-a_3a_4)_K\\ &\Leftrightarrow \forall x\in K^\times,(x,a_1a_2a_3a_4)_K=1\\ &\Leftrightarrow \forall x\in K^\times,(x,\mathrm{disc}(q))_K=1\\ &\Leftrightarrow \mathrm{disc}(q)\in K^{\times2}\end{aligned}$$

Ainsi, q ne représente pas 0 si et seulement si $(a_1,a_2)_K=-(-a_3,-a_4)_K$ et $\mathrm{disc}(q)\in K^{\times2}$. Or, si $\mathrm{disc}(q)\in K^{\times2}$, $(a_1a_2,a_3a_4)_K=(a_3a_4,a_3a_4)_K$ et donc

$$\begin{aligned}c_K(f)&=(a_1,a_2)_K,(a_1,a_3)_K,(a_1,a_4)_K(a_2,a_3)_K,(a_2,a_4)_K,(a_3,a_4)_K\\ &=(a_1,a_2)_K(a_3,a_4)_K(a_1a_2,a_3a_4)_K\\ &=(a_1,a_2)_K(a_3,a_4)_K(a_3a_4,a_3a_4)_K\\ &=(a_1,a_2)_K(a_3,a_4)_K(-1,a_3a_4)_K\\ &=(a_1,a_2)_K(-a_3,-a_4)_K(-1,-1)_K.\end{aligned}$$

Et donc q ne représente pas 0 si et seulement si $c_K(f)=-(-1,-1)_K$ et $\mathrm{disc}(q)\in K^{\times2}$. Par contraposition, on a le résultat annoncé.

Si $\underline{n=5}$. Le cas réel est une conséquence directe de la classification des formes quadratiques réelles. On s'intéresse donc au cas p-adique. On note $q_1=a_1x_1^2+a_2x_2^2$ et que $q=q_1\oplus(a_3x_3^2+a_4x_4^2+a_5x_5^2)$. Si $-\mathrm{disc}(q_1)$ est un carré, par le cas $n=2$, q_1 représente

0 puis q également. On suppose donc que $-a_1a_2$ n'est pas un carré. Soit $x \in \mathbb{Q}_p^\times$, le lemme 4.47 montre que q_1 représente x si et seulement si $(x, -\text{disc}(q_1))_K = (a_1, a_2)_K$. Et comme $-\text{disc}(q_1)$ n'est pas un carré, ceci arrive pour x dans la moitié des classes modulo $x \in \mathbb{Q}_p^{\times 2}$. Comme $[\mathbb{Q}_p : \mathbb{Q}_p^{\times 2}]$ vaut 4 ou 8, au moins deux classes sont représentées par q_1, et donc il existe $a \in \mathbb{Q}_p^\times$ représenté par q_1 et dans une classe distincte de $\text{disc}(q)$. Par la proposition 4.23, on peut alors écrire $q = q' \oplus ax^2$ avec q' de dimension 4. Comme $\text{disc}(q) = a\text{disc}(q')$ et que a n'est pas dans la classe de $\text{disc}(q)$, $\text{disc}(q')$ n'est pas un carré et donc par le cas $n = 4$, q' représente 0 puis q également. □

Corollaire 4.52. *Soit $K = \mathbb{R}$ ou $\mathbb{Q}_p$. Soit (E, q) un K-espace quadratique de dimension n avec q non dégénérée. Pour que q représent $a \in K^\times$, il faut et il suffit qu'une des conditions suivantes soit réalisée :*

- *$n = 1$ et $disc(q)/a \in K^{\times 2}$;*
- *$n = 2$ et $(a, -d(q))_K = c_K(q)$;*
- *$n = 3$ et $(-disc(q)/a \notin K^\times$ ou $(-1, -disc(q))_K = c_K(q))$;*
- *$n \geq 4$ et si $K = \mathbb{R}$ que la première (resp. seconde) coordonnée de la signature de q soit non nulle et $a > 0$ (resp. $a < 0$).*

Démonstration. q représente $a \in K^\times$ si et seulement si $q \ominus ax^2$ représente 0 par le lemme 4.22. On applique donc le théorème précédent à $q \ominus ax^2$.

Si $\underline{n = 1}$, alors la condition équivalente est $-\text{disc}(q \ominus ax^2) \in K^{\times 2}$, c'est à dire $\text{disc}(q)a \in K^{\times 2}$, ou encore, $\text{disc}(q)/a \in K^{\times 2}$.

Le cas $\underline{n = 2}$ correspond au lemme 4.47.

Si $\underline{n = 3}$, alors la condition équivalente est $(\text{disc}(q \ominus ax^2) \notin K^{\times 2}$ ou $(-1, -1)_K = c_K(q \ominus ax^2))$, c'est à dire $(-\text{disc}(q)/a \notin K^{\times 2}$ ou $(-1, -1)_K = c_K(q)(\text{disc}(q), -a)_K)$. Or si première condition n'est pas remplie, la seconde équivaut à $(\text{disc}(q), -a)_K = (\text{disc}(q), \text{disc}(q))_K = (-1, \text{disc}(q))_K$ et donc q représente a si et seulement si $(-\text{disc}(q)/a \notin K^\times$ ou $(-1, -\text{disc}(q))_K = c_K(q))$.

Si $\underline{n = 4}$, c'est une conséquence immédiate du théorème précédent. □

Théorème 4.53 (Classification des formes quadratiques sur $\mathbb{Q}_p$)**.** *Deux formes quadratiques p-adiques non dégénérées sont équivalentes si et seulement si elles ont même rang, même discriminant et même symbole de Hasse.*

Démonstration. On a montré précédemment que les différentes quantités évoquées étaient bien des invariants des classes d'équivalence.

Réciproquement, on va montrer par récurrence sur $n \in \mathbb{N}$ que si q_1 et q_2 sont non dégénérées, ont même rang n, même symbole de Hasse et même discriminant, elles sont équivalentes. Le cas $n = 0$ est trivial. Supposons le résultat au rang $n - 1$. La proposition montre que q_1 et q_2 représentent les mêmes nombres. Soit donc $a \in K^\times$ représenté par q_1 et q_2. On peut écrire $q_1 = ax^2 \oplus q_1'$ et $q_2 = ax^2 \oplus q_2'$ par la proposition 4.23. Alors q_1' et q_2' sont de rang $n - 1$, $\text{disc}(q_1') = \text{disc}(q_1)/a = \text{disc}(q_2)/a = \text{disc}(q_2')$ et $c_K(q_1') = c_K(q_1)/(\text{disc}(q_1'), a)_K = c_K(q_2)/(\text{disc}(q_2'), a)_K = c_K(q_2')$, ce qui permet d'appliquer l'hypothèse de récurrence et conclut. □

4.5 Théorème de Hasse-Minkowski et applications

Le but de cette partie est de démontrer le résultat fondamental suivant.

Théorème 4.54 (Hasse-Minkowski)**.** *Soit q une forme quadratique rationnelle. Alors q représente 0 sur $\mathbb{Q}$ si et seulement si elle représente 0 sur $\mathbb{R}$ et sur tous les $\mathbb{Q}_p$.*

4.5.1 Preuve du théorème

La preuve donnée ici est adaptée de [4, p.126] et [11, p.41].

Notons déjà que le sens direct est automatique car $\mathbb{Q}$ est inclus dans $\mathbb{R}$ et dans les $\mathbb{Q}_p$. Il s'agit donc de montrer le sens réciproque. Soit q une forme quadratique rationnelle qui représente 0 sur $\mathbb{R}$ et les $\mathbb{Q}_p$. Si q est une forme quadratique dégénérée, elle représente 0 donc on peut la supposer non dégénérée. De plus, quitte à la remplacer par une forme équivalente, on peut considérer la forme quadratique définie sur $\mathbb{R}^n$ par $q(x) = a_1x_1^2 + \ldots + a_nx_n^2$ avec $a_1, \ldots, a_n \in \mathbb{Q}^\times$. Finalement q représente 0 si et seulement si q/a_1 représente 0 et on peut donc supposer que $a_1 = 1$ si nécessaire. On va maintenant faire une disjonction de cas en fonction de la valeur de n qu'on peut prendre supérieure ou égale à 2 car une forme non dégénérée de rang 1 ne représente pas 0.

Cas $n = 2$

On écrit $q = x_1^2 - a_2x_2^2$ avec $a_2 \in \mathbb{Q}^\times$. Comme q représente 0 sur $\mathbb{R}$, $a_2 > 0$ et on a donc $a_2 = \prod_{p\in\mathcal{P}} p^{v_p(a_2)}$. Pour tout nombre premier p, comme q représente 0 sur $\mathbb{Q}_p$, a_2 est un carré de $\mathbb{Q}_p^\times$ et donc $v_p(a)$ est pair. Ainsi, $a_2 = \Big(\prod_{p\in\mathcal{P}} p^{v_p(a_2)/2}\Big)^2$ est le carré d'un rationnel et donc q représente 0 sur $\mathbb{Q}$.

Cas $n = 3$

On écrit $q = x_1^2 - a_2x_2^2 - a_3x_3^2$. Quitte à remplacer q par une forme équivalente en multipliant a_2 par a_3 par des carrés, on peut supposer que a_2 et a_3 sont des entiers sans facteurs carrés et quitte à les échanger, on a $|a_2|_\infty \leq |a_3|_\infty$. On va maintenant entamer un procédé de descente afin de se ramener à $|a_3|_\infty \leq 1$. Sous cette dernière condition, la forme q s'écrira $x_1^2 \pm x_2^2 \pm x_3^2$ avec au moins un des $\pm$ valant $-$ car q représente 0 sur $\mathbb{R}$ et une forme quadratique de cette forme représente bien 0 sur $\mathbb{Q}$.

On suppose donc $|a_2|_\infty \geq 2$ et on écrit $a_3 = \pm\prod_{i=1}^{s} p_i$ où les p_i sont des premiers distincs. Soit $i \in [\![1, s]\!]$, ou bien $a_2 \equiv 0[p_i]$ et est donc un carré dans $\mathbb{F}_{p_i}$. Ou bien comme q représente 0 dans $\mathbb{Q}_{p_i}$, il existe $x, y, z \in \mathbb{Q}_p$ non tous nuls tels que $a_2x^2 + a_3y^2 = z^2$. Comme on a $v_{p_i}(a_2) = 0$ et $v_{p_i}(a_3) = 1$, et de la même façon que dans la preuve du cas p impair de la proposition 4.39, on en déduit que a_2 est un carré dans $\mathbb{F}_{p_i}$. Par le théorème des restes chinois, a_2 est donc un carré modulo $\prod_{i=1}^{s} p_i$. Ainsi, il existe $t \in \mathbb{Z}$ tel que $t^2 \equiv a_2[a_3]$ et on peut de plus supposer $|t|_\infty \leq \frac{|a_3|_\infty}{2}$ quitte à remplacer t par

un t' dans cet intervalle tel que $t' \equiv t[a_3]$. On peut donc écrire $t^2 - a_2 = a_3 a_3'$ avec $a_3' \in \mathbb{Z}$. Soit K un corps contenant $\mathbb{Q}$, la forme $x_1^2 - a_2 x_2^2$ représente donc $a_3 a_3'$ sur K. Ainsi, q représente 0 sur K si et seulement si $x_1^2 - a_2 x_2^2$ représente a_3 sur K si et seulement si $x_1^2 - a_2 x_2^2$ représente $a_3' = \frac{a_3 a_3'}{a_3}$ sur K par la proposition 4.38, si et seulement si $q' := x_1^2 - a_2 x_2^2 - a_3' x_3'^2$ représente 0 sur K. Ainsi, la forme q' représente 0 sur tous les $\mathbb{Q}_p$ et sur $\mathbb{R}$, et il s'agit de montrer qu'elle représente 0 sur $\mathbb{Q}$. De plus, comme $|a_3|_\infty \geq 2$, on a

$$|a_3'|_\infty = \frac{|t^2 - a_2|_\infty}{|a_3|_\infty} \leq \frac{|t^2|_\infty}{|a_3|_\infty} + \frac{|a_2|_\infty}{|a_3|_\infty} \leq \frac{|a_3|_\infty}{4} + 1 < |a_3|_\infty.$$

Ainsi, quitte à permuter a_3' et a_2, on se ramène à une forme $q'' = x_1^2 - a_2'' x_2^2 - a_3'' x_3^2$ avec $(a_3'', a_3'') < (a_3, a_2)$ dans l'ordre lexicographique, ce qui permet d'effectuer le processus de descente et conclut.

Cas $n = 4$

On écrit $q = a_1 x_1^2 + a_2 x_2^2 - a_3 x_3^2 - a_4 x_4^2$. Soit K un corps contenant $\mathbb{Q}$. Alors q représente 0 sur K si et seulement si $q_1 := a_1 x_1^2 + a_2 x_2^2$ et $q_2 := a_3 x_3^2 + a_4 x_4^2$ représentent une même valeur $y \in K^\times$. Soit $v \in V$ avec V l'ensemble des nombres premiers auquel on a adjoint $+\infty$. Comme q représente 0 sur $\mathbb{Q}_v$, il existe $y_v \in \mathbb{Q}_v^\times$ représenté par q_1 et q_2. Par la proposition 4.52, on a $(y_v, -a_1 a_2)_v = (a_1, a_2)_v$ et $(y_v, -a_3 a_4)_v = (a_3, a_4)_v$. Les hypothèses de la proposition 4.44 sont alors vérifiées et il existe $y \in \mathbb{Q}^\times$ tel que pour tout $v \in V$, $(y, -a_1 a_2)_v = (a_1, a_2)_v$ et $(y, -a_3 a_4)_v = (a_3, a_4)_v$. En particulier, q_1 et q_2 représentent y sur tous les $\mathbb{Q}_v$ puis $q_1 \ominus yx^2$ et $q_2 \ominus yx^2$ représentent 0 sur tous les $\mathbb{Q}_v$, donc sur $\mathbb{Q}$ par le cas $n = 3$ du théorème de Hasse-Minkowski. Ainsi q_1 et q_2 représente y sur $\mathbb{Q}$ et donc q représente 0 sur $\mathbb{Q}$.

Cas $n = 5$

On écrit $q = q_1 \ominus q_2$ avec $q_1 = x_1^2 + a_2 x_2^2$ et $q_2 = a_3 x_3^2 + a_4 x_4^2 + a_5 x_5^2$. Alors q représente 0 sur K si et seulement si q_1 et q_2 représentent une même valeur $y \in K^\times$. Soit $S = \{p \in \mathcal{P}, \exists i \in [\![1, 5]\!], v_p(a_i) \neq 0\} \cup \{2, \infty\}$. Soit $v \in S$, comme q représente 0 sur $\mathbb{Q}_v$, il existe $y_v \in \mathbb{Q}_v^\times$ représenté par q_1 et q_2, on peut en particulier prendre x_1^v et x_2^v dans $\mathbb{Q}_v$ tels que $y_v = a_1 (x_1^v)^2 + a_2 (x_2^v)^2$. Comme les $y_v \mathbb{Q}_v^{\times 2}$ sont des ouverts, par le théorème d'approximation 1.15, on peut prendre x_1 et x_2 dans $\mathbb{Q}^\times$ tels que pour tout $v \in S$, x_1 (resp. x_2) soient suffisamment proches de x_1^v et (resp. x_2^v) dans $\mathbb{Q}_v$ afin que $y := a_1 x_1^2 + a_2 x_2^2 \in y_v \mathbb{Q}_v^{\times 2}$. Pour $v \in S$, comme $y \in y_v \mathbb{Q}_v^{\times 2}$ et que y_v est représenté par q_2, y est également représenté par q_2. Si maintenant $v \in V \backslash S$ comme a_3, a_4 et a_5 vérifient $v_v(a_i) = 0$, ils sont dans $\mathbb{Z}_v^\times$ donc $\mathrm{disc}(q_2) \in \mathbb{Z}_v^\times$ et comme p est impair, par la proposition 4.41 $c_p(q_2) = 1$. On a donc $(-1, -\mathrm{disc}(q_2)) = c_v(q_2)$ et q_2 représente donc y sur $\mathbb{Q}_v$ par le corollaire 4.52. Ainsi, pour tout $v \in V$, $q_2 \ominus yx^2$ représente 0 sur $\mathbb{Q}_v$, puis par le cas $n = 4$ du théorème de Hasse-Minkowski $q_2 \ominus yx^2$ représente 0 sur $\mathbb{Q}$. Ainsi q_2 représente a sur $\mathbb{Q}$ et comme c'est également le cas de q_1, $q = q_1 \ominus q_2$ représe 0 sur $\mathbb{Q}$.

Cas $n \geq 6$

On écrit $q = \sum_{i=1}^{n} a_i x_i^2$. Comme q représente 0 sur $\mathbb{R}$, au moins un des a_i est positif et au moins un négatif. Quitte à permuter les a_i, on suppose $a_1 > 0$ et $a_2 < 0$. La forme $q' = \sum_{i=1}^{5}$ représente donc 0 sur $\mathbb{R}$ et par le théorème 4.51 q' représente 0 sur $\mathbb{Q}_p$. Par le cas $n = 5$ du théorème de Hasse-Minkowski, q' représente 0 sur $\mathbb{Q}$ et donc q aussi.

4.5.2 Formes quadratiques sur $\mathbb{Q}$

Voici quelques conséquences du théorème de Hasse-Minkowski qui permettent de classifier les formes quadratiques rationnelles.

Corollaire 4.55. *Soit q une forme quadratique rationnelle non dégénérée et $a \in \mathbb{Q}^\times$. Alors q représente a sur $\mathbb{Q}$ si et seulement si elle représente 0 sur $\mathbb{R}$ et sur tous les $\mathbb{Q}_p$.*

Démonstration. Soit K un corps contenant $\mathbb{Q}$. Par la proposition 4.22, q réprésente a sur K si et seulement si $q \ominus ax^2$ représente 0 sur K. On peut alors appliquer le théorème de Hasse-Minkowski à $q \ominus ax^2$, ce qui conclut. □

Théorème 4.56 (Classification des formes quadratiques sur $\mathbb{Q}$)**.** *Deux formes quadratiques rationnelles non dégénérées sont équivalentes sur $\mathbb{Q}$ si et seulement si elles le sont sur $\mathbb{R}$ et sur tous les $\mathbb{Q}_p$.*

Démonstration. Le sens direct est immédiat. Montrons le sens réciproque par récurrence sur le rang des formes quadratiques. Si q_1 et q_2 sont de rang 0 le résultat est clair. Si q_1, q_2 sont de rang n et équivalentes sur tous les $\mathbb{Q}_v$ avec $v \in V$, elles représentent les mêmes valeurs sur les $\mathbb{Q}_v$ et donc sur $\mathbb{Q}$ d'après le théorème de Hasse-Minkowski. Soit alors $a \in \mathbb{Q}^\times$ représenté par q_1 et q_2, on peut prendre q_1' et q_2' des formes quadratiques rationnelles non dégénérées de rang $n-1$ tel que $q_i = q_i' \oplus ax^2$ pour $i \in \{1, 2\}$. On a alors $q_1' + ax^2 \sim q_2' + ax^2$ sur tous les $\mathbb{Q}_v$ donc par le théorème de Witt, $q_1' \sim q_2'$ sur tous les $\mathbb{Q}_v$, puis par hypothèse de récurrence sur $\mathbb{Q}$ et donc $q_1 \sim q_2$. □

A partir du théorème précédent et des classifications des formes quadratiques sur $\mathbb{Q}_p$ et $\mathbb{R}$, on obtient aussitôt le corollaire suivant.

Corollaire 4.57. *Deux formes quadratiques rationnelles non dégénérées sont équivalentes sur $\mathbb{Q}$ si elles ont même discriminant, même symbole de hasse pour tout nombre premier p et même signature.*

4.5.3 Somme de carrés

A titre d'application du théorème de Hasse-Minkowski, on propose dans cette section de s'intéresser aux entiers sommes de deux, trois ou quatre carrés. On suit [4, p.134].

Le théorème de Hasse-Minkoswki nous renseigne sur les rationnels représentés par une forme quadratique rationnelle. Dans le cas où la forme quadratique est à coefficients entiers (on parle alors de forme quadratique entière), il est légitime de se poser la question des entiers qu'elle représente sur $\mathbb{Z}$. Le théorème suivant nous permet de traiter quelques cas (rares) cas de représentation d'un entier sur $\mathbb{Z}$ par une forme quadratique entière.

Théorème 4.58 (Davenport-Cassels)**.** *Soit q une forme quadratique entière non dégénérée de rang n. On suppose que q ne représente pas 0 sur $\mathbb{Q}$ et que pour tout $x \in \mathbb{Q}^n$, il existe $y \in \mathbb{Z}^n$ tel que $|q(x-z)|_\infty < 1$. Alors pour tout $a \in \mathbb{Z}$ représenté par q sur $\mathbb{Q}$, il existe $z \in \mathbb{Z}^n$ tel que $q(z) = a$.*

Démonstration. Soit $x \in \mathbb{Q}^n$ tel que $q(x) = a$. On peut écrire $x = \frac{r}{d}$ avec $r \in \mathbb{Z}^n$ et $d \in \mathbb{Z}\backslash\{0\}$. Par hypothèse, il existe également $y \in \mathbb{Z}^n$ tel que $|q(x-s)|_\infty < 1$. Si $x = s$, il suffit de prendre $z = x$. Sinon, comme q ne représente pas 0 sur $\mathbb{Q}$, $0 < |q(x-s)|_\infty < 1$. On va maintenant entamer un processus de descente. Pour cela, on commence par chercher $\alpha, \beta \in \mathbb{Z}$ tels que $r' := \alpha r + \beta s$ et $d' := \alpha d + \beta$, on ait $f(\frac{r'}{d'}) = a$ et $d' = dq(x-s)$. On a

$$\begin{aligned} f(r') &= \alpha^2 q(r) + \beta^2 q(s) + 2\alpha\beta B_q(r,s) \\ &= \alpha^2 d^2 a + \beta^2 q(s) + 2\alpha\beta B_q(r,s) \\ &= d'^2 a + \beta^2(q(s) - a) + 2\alpha\beta(B_q(r,s) - da) \end{aligned}$$

et

$$\begin{aligned} d^2 q(x-s) &= q(r - ds) \\ &= d^2\alpha^2 + d^2 q(s) + 2dB_q(r,s) \\ &= d(\alpha d + \beta) + d^2(q(s) + a - \alpha) - d(2B_q(r,s) + \beta). \end{aligned}$$

On obtient les égalités voulues pour $\alpha = q(s) - a$ et $\beta = 2(da - B_q(r,s))$. L'encadrement $0 < |q(x-s)|_\infty < 1$ entraine $0 < |d'|_\infty < |d|_\infty$, ce qui permet de réaliser la descente jusqu'à obtenir $|d|_\infty = 1$ et $z = \frac{r}{d}$ est alors un entier qui convient. □

Théorème 4.59 (Théorème des deux carrés)**.** *Soit $a \in \mathbb{N}^*$, alors a est somme de deux carrés entiers si et seulement si pour tout nombre premier $p \equiv 3[4]$, $v_p(a)$ est pair.*

Démonstration. Il s'agit de considérer les entiers représentés sur $\mathbb{Z}$ par $q(x_1, x_2) = x_1^2 + x_2^2$. Pour $x_1, x_2 \in \mathbb{Q}$ on peut prendre $x_1', x_2' \in \mathbb{Z}$ tel que pour $i \in \{1,2\}$, $|x_i - x_i'| \leq \frac{1}{2}$ de sorte que $q(x - x') \leq \frac{1}{2} < 1$. q vérifie donc les hypothèse du théorème de Davenport-Cassels et a est représenté par q sur $\mathbb{Z}$ si et seulement il est représenté par q sur $\mathbb{Q}$ si et seulement il est représenté par q sur tous les $\mathbb{Q}_p$ d'après le théorème de Minkowski. Par la proposition 4.52, ceci équivaut à

$$\forall v \in V, (a, -\mathrm{disc}(q))_v = c_v(q),$$

équation qui se réécrit ici $(a,-1)_v = 1$. Pour $v = \infty$, cette condition est automatiquement remplie. Pour v impair, celle ci équivaut à $(a',-1)_v = 1$ où $a = a'b^2$ avec a' sans facteur carré. Si v ne divise pas a', a' est une unité v-adique et $(a',-1)_v = 1$. Sinon,

$$(a',-1)_v = (v,-1)_v = \left(\frac{-1}{v}\right) = (-1)^{\frac{v-1}{4}}.$$

Ainsi, a est somme de carrés si et seulement $v_p(a') = 0$ pour $p \equiv 3[4]$, ce qui revient à $v_p(a)$ est pair. □

Notons qu'on n'a pas évoqué le cas $v = 2$ dans cette preuve. En effet, si les symboles de Hilbert valent 1 pour tous $v \in V\backslash\{2\}$, la loi de réciprocité de Hilbert donne que c'est également le cas pour $v = 2$.

Théorème 4.60 (Théorème des trois carrés)**.** *Soit $a \in \mathbb{N}^*$, alors a est somme de trois carrés entiers si et seulement s'il n'est pas de la forme $4^l(8k+7)$ avec $l \in \mathbb{N}$ et $k \in \mathbb{Z}$.*

Démonstration. Comme dans la preuve précédente, $q = x_1^2 + x_2^2 + x_3^2$ vérifie les conditions du théorème de Davenport-Cassels et par le théorème de Hasse Minkowski et la proposition 4.52, a est somme de trois carrés si et seulement si

$$\forall v \in V, (-1,-1)_v = 1 \text{ ou } -1/a \notin \mathbb{Q}_v^{\times 2}.$$

La première condition est vérifiée pour tout v impair et ne l'est pas pour $v = 2$ et la seconde est vérifiée pour $v = \infty$. Ainsi a est somme de trois carrés si et seulement si $-1/a \notin \mathbb{Q}_v^{\times 2}$. a n'est donc pas somme de 3 carré si et seulement si $-a \in \mathbb{Q}_v^{\times 2}$, ce qui par la classification des carrés de $\mathbb{Q}_2^\times$ équivaut à $v_2(a)$ pair et $-a2^{v_2(a)} \in \mathbb{Z}_2^{\times 2} = 1 + 8\mathbb{Z}_2$ ou encore $a = 4^l(8k+7)$ avec $l \in \mathbb{N}^*$ et $k \in \mathbb{Z}$. □

Théorème 4.61 (Théorème des quatre carrés)**.** *Tout entier naturel est somme de quatre carrés d'entiers.*

Démonstration. Si a est somme de 3 carrés, il est somme de 4 carrés car $a = a + 0^2$. Sinon, $a = 4^h(8k+7) = 4^h(8k+6) + (2^h)^2$ et comme $4^h(8k+6)$ est somme de 3 carrés, a est somme de quatre carrés. □

Références

[1] Nicolas Bourbaki. *Algèbre Commutative, chapitres 5 à 7.* Éléments de Mathématique. Springer, 2006.

[2] Keith Conrad. *Ostrowski for number fields.* URL : `https://kconrad.math.uconn.edu/blurbs/gradnumthy/ostrowskinumbfield.pdf`.

[3] Keith Conrad. *Ostrowski's theorem for F(T).* URL : `https://kconrad.math.uconn.edu/blurbs/gradnumthy/ostrowskiF(T).pdf`.

[4] Roger Descombes. *Éléments de théorie des nombres.* Presses Universitaires de France, 1986.

[5] J.W.S. Cassels ; A. Fröhlich. *Algebraic Number Theory.* Academic Press, 1967.

[6] Adam Gamzon. *The Hasse-Minkowski Theorem.* URL : `https://digitalcommons.lib.uconn.edu/cgi/viewcontent.cgi?article=1017&context=srhonors_theses`.

[7] P. Caldero ; J. Germoni. *Histoires hédonistes de groupes et géométries.* Calvage-et-Mounet, 2016.

[8] Fernando Q. Gouvêa. *p-adic Numbers.* Universitext. Springer, 2020.

[9] Serge Lang. *Algebraic Number Theory*. Graduate Texts in Mathematics. Springer, 1994.

[10] Pierre Samuel. *Théorie algébrique des nombres*. Hermann, 1971.

[11] J.P. Serre. *Cours d'arithmétique*. Presses Universitaires de France, 1994.

[12] Tristan Vaccon. *Théorie du corps de classes local*. 2011. URL : `https://www.unilim.fr/pages_perso/tristan.vaccon/rapport2011.pdf`.