# Le théorème de Hasse-Minkowski

Yicheng Zhou

## Table des matières

*Convention/Notation :* (i) On suppose que les corps et les anneaux sont *commutatifs*.

(ii) On munit un espace produit d'espaces topologiques toujours de la *topologie produit*.

(iii) Soit $A$ un anneau, on note $A^n$ pour l'ensemble des $n$-uplets à composantes dans $A$ ; soit $k$ un corps, on note $k^{\times 2}$ pour $\{x^2 : x \in k^\times\}$ l'ensemble des carrés non zéros dans $k^\times$.

(iv) Soit $A$ un anneau. On dit qu'une solution dans $A^n$ d'une équation polynomiale à $n$ variables est *non zéro* si toutes ses composantes ne s'annulent pas.

# 0 Introduction

Dans ce mémoir, on présentera le théorème Hasse-Minkowski, qui fournit un premier exemple du principe local-global.

Au sens usuel, une *forme quadratique* sur $k$ est un polynôme homogène de degré 2 à coefficients dans $k$. Pour les extensions de corps $K/\mathbb{Q}$, par exemple pour $K = \mathbb{R}$ ou $\mathbb{Q}_p$ (2.1.6), on peut naturellement voir $f$ comme une forme quadratique sur $K$. S'il existe une solution non zéro de $f = 0$ dans $\mathbb{Q}^n$, il en est aussi dans $K^n$ ; la réciproque est fausse en général, mais elle sera vraie si on considère en même temps les extensions $\mathbb{Q}_p$ et $\mathbb{R}$ de $\mathbb{Q}$ :

**Théorème** (Hasse-Minkowski). *Soit $f$ une forme quadratique sur $\mathbb{Q}$ à $n$ variables. $f = 0$ admet une solution non zéro dans $\mathbb{Q}^n$ si et seulement si $f = 0$ admet une solution non zéro dans $\mathbb{R}^n$ et dans $\mathbb{Q}_p^n$ pour tout nombre premier $p$.*

On en verra une reformulation après (2.4.5).

La nécessité sera évidente quand on aura vu la définition de $\mathbb{Q}_p$ (2.1.6). La suffisance est plus difficile et non triviale. On présentera dans la suite les formes quadratiques, les nombres $p$-adiques et le symbole de Hilbert. On démontra de temps en temps certains cas du théorème en utilisant différentes facettes de ces théories. Enfin, après avoir démontré le théorème, on donnera une classification de formes quadratiques sur $\mathbb{R}$ et $\mathbb{Q}_p$ par des invariants.

# 1 Formes quadratiques : généralités

Soit $k$ un corps de caractéristique $\neq 2$. Tous les $k$-espaces vectoriels considérés seront de dimension *finie*.

## 1.1 Définitions

**1.1.1 (Forme quadratique et espace quadratique).** Soit $V$ un espace vectoriel sur $k$. Une application $Q : V \to k$ est appelée une *forme quadratique sur $V$* si

(i) On a $Q(ax) = a^2 Q(x)$ pour $a \in k$ et $x \in V$.

(ii) L'application $(x, y) \mapsto x \cdot y := \frac{1}{2}\Big(Q(x+y) - Q(x) - Q(y)\Big)$ est une forme $k$-bilinéaire.

Un tel couple $(V, Q)$ (ou simplement $V$) est appelé un *espace quadratique* sur $k$.

**1.1.2** (**Produit scalaire**). Soit $(V, Q)$ un espace quadratique sur $k$. L'application $(x, y) \mapsto x \cdot y$ définie ci-dessus est une forme $k$-bilinéaire symétrique ; on l'appelle le *produit scalaire* sur $V$ associé à $Q$ ; en posant $y = x$, on retrouve $Q$ par $Q(x) = x \cdot x$.

Inversement, si on se donne $B(\cdot, \cdot)$, une forme $k$-bilinéaire symétrique sur $V$, on pourra lui associer une application $Q_B(x) = B(x, x)$. On vérifie bien que $Q_B$ satisfait (i), (ii), et $Q_B$ est donc une forme quadratique sur $V$. Le produit scalaire associé est

$$(x, y) \mapsto \frac{1}{2}\big(B(x + y, x + y) - B(x, x) - B(y, y)\big) = \frac{1}{2}\big(B(x, y) + B(y, x)\big) = B(x, y)$$

par la bilinéarité et la symétricité de $B(\cdot, \cdot)$.

Ainsi, $Q \rightsquigarrow x \cdot y$, $Q_B \leftsquigarrow B(x, y)$ sont des inverses l'une de l'autre, établissant une correspondance bijective entre formes quadratiques et formes bilinéaires symétriques sur $V$.

**1.1.3** (**Matrice d'une forme quadratique**). Soit $(V, Q)$ un espace quadratique sur $k$. Soit $\mathscr{E} = (e_i)_{1 \le i \le n}$ une base de $V$. On appelle *matrice de* $Q$ par rapport à cette base la matrice $A_{\mathscr{E}} = (e_i \cdot e_j)_{1 \le i,j \le n}$, qui est une matrice symétrique (1.1.2). Pour $x = \sum_i X_i e_i \in V$, on a par la bilinéarité $Q_{\mathscr{E}}(X) := \big(\sum_i X_i e_i\big) \cdot \big(\sum_j X_j e_j\big) = \sum_{i,j} a_{ij} X_i X_j$ ; $Q_{\mathscr{E}}$ ainsi définie est une forme quadratique en $X = (X_1, \ldots, X_n)$ au sens *usuel*. Soit $\mathscr{E}' = (e'_i)_{1 \le i \le n}$ une autre base de $V$. Il existe alors une matrice $P = (p_{ij}) \in \mathrm{GL}_n(k)$ telle que $e'_i = \sum_k p_{ki} e_k$, d'où

$$A_{\mathscr{E}'} = \Big(\sum_{k,l} p_{ki} e_k \cdot p_{lj} e_l\Big)_{i,j} = (p_{ki})_{i,k} (e_k \cdot e_l)_{k,l} (p_{lj})_{l,j} = {}^t P A_{\mathscr{E}} P \tag{1.1.3.1}$$

**1.1.4** (**Morphisme métrique et isomorphisme**). Soient $(V, Q)$ et $(V', Q')$ deux espaces quadratiques. Un *morphisme (métrique)* de $(V, Q)$ dans $(V', Q')$ est une application linéaire $f : V \to V'$ telle que $Q' \circ f = Q$ sur $V$, ou ce qui revient au même (1.1.2) de dire que $f(x) \cdot f(y) = x \cdot y$ pour $x, y \in V$ ; $f$ est dit un *isomorphisme* si elle est bijective, et on note alors $(V, Q) \simeq (V', Q')$, ou simplement $V \simeq V'$ ou $Q \simeq Q'$. On en déduit que si $f : V \to V'$ est un isomorphisme et si $\mathscr{E}$ est une base de $V$, $f(\mathscr{E})$ est une base de $V'$ et la matrice de $Q$ par rapport à $\mathscr{E}$ est égale à la matrice de $Q'$ par rapport à $f(\mathscr{E})$. La relation d'isomorphisme est une relation d'équivalence entre espaces quadratiques.

**1.1.5** (**Discriminant : un invariant**). Un *invariant* des espaces quadratiques sur $k$ est une quantité associée à chaque espace quadratique sur $k$ qui ne dépend que de sa classe d'isomorphisme. Introduisons ici un invariant qui s'appelle le discriminant. Nous verrons d'autres invariants dans (1.4.4) et dans (3.4.1.1).

Soit $(V, Q)$ un espace quadratique sur $k$. Avec la notation de (1.1.3), on déduit de (1.1.3.1) que $\det A_{\mathscr{E}'} = \big(\det P\big)^2 \det A_{\mathscr{E}}$. Donc la classe de $\det A_{\mathscr{E}}$ dans $k^\times / k^{\times 2} \cup \{0\}$ ne dépend pas de la base $\mathscr{E}$ choisie ; cette classe est notée $d(Q)$ et est appelée le *discriminant* de $(V, Q)$. Selon (1.1.4), $d(Q) = d(Q')$ si $(V, Q)$ et $(V', Q')$ sont isomorphes ; $d(Q)$ est donc un invariant associé à $(V, Q)$.

**1.1.6.** On dit que $Q$ *représente* un élément $a \in k$ s'il existe $x \in V$ non zéro tel que $Q(x) = a$. Comme on a (1.1.1) $Q(0 \cdot x) = 0^2 \cdot Q(x) = 0$, la condition « non zéro » est redondante si $a \in k^\times$. Il est clair que si $(V, Q) \simeq (V, Q')$, $Q$ et $Q'$ représentent les mêmes éléments dans $k$.

## 1.2 Orthogonalité

Soit $(V, Q)$ un espace quadratique sur $k$.

**1.2.1.** Deux éléments $x, y \in V$ sont dits *orthogonaux* si $x \cdot y = 0$. Pour toute partie $A$ de $V$, on note $A^\perp := \{x \in V : x \cdot y = 0 \text{ pour tout } y \in V\}$. On appelle $\mathrm{Rad}(V) := V^\perp$ le *radical* de $V$. On dit que $(V, Q)$ (ou simplement $V$) est *non dégénéré* si $\mathrm{Rad}(V) = 0$. Pour tout sous-espace vectoriel $U$ de $V$, le couple $(U, Q|_U)$ est un espace quadratique. On dit que le sous-espace $U$ est *non dégénéré* si $(U, Q|_U)$ est non dégénéré. La non dégénérescence est invariante sous isomorphismes d'espaces quadratiques.

Deux sous-espaces vectoriels $V_1, V_2$ de $V$ sont dits *orthogonaux* si $V_1 \subset V_2^\perp$, ou de manière équivalente si $V_2 \subset V_1^\perp$. Soient $U_1, \ldots, U_m$ des sous-espaces vectoriels de $V$, on dit que $V$ est la *somme directe orthogonale* des $U_i$ si ceux-ci sont deux à deux orthogonaux et si $V$ en est la somme directe ; on écrit alors

$$V = U_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} U_m$$

Une base $\mathscr{E} = (e_i)_{1 \le i \le n}$ de $(V, Q)$ est appelée *base orthogonale* si $V = ke_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} ke_n$. On verra qu'une telle base existe toujours (1.2.3).

**1.2.2 - Proposition.** *(i) Soient $U_1, U_2$ deux parties de $V$ telles que $U_1 \subset U_2$. On a $U_2^\perp \subset U_1^\perp$.*

*(ii) Supposons $V$ non dégénéré. Soit $U$ un sous-espace vectoriel de $V$. On a $(U^\perp)^\perp = U$. Si de plus $U$ est non dégénéré, $U^\perp$ est non dégénéré et $V = U \overset{\perp}{\oplus} U^\perp$.*

*Démonstration.* (i) On a $U_1 \subset U_2 \subset (U_2^\perp)^\perp$, donc $U_2^\perp$ et $U_1$ sont orthogonaux, donc $U_2^\perp \subset U_1^\perp$.

(ii) La non dégénérescence de $V$ implique $\dim U + \dim U^\perp = \dim V$. En remplaçant $U$ par $U^\perp$, on obtient $\dim U^\perp + \dim (U^\perp)^\perp = \dim V$. Donc $\dim (U^\perp)^\perp = \dim U$. Or, on a $U \subset (U^\perp)^\perp$, d'où $U = (U^\perp)^\perp$ en raison de la dimension.

De la définition du radical (1.2.1), on déduit que $\mathrm{Rad}(U) = \mathrm{Rad}(U^\perp) = U \cap U^\perp$. Si $U$ est non dégénéré, on a $\mathrm{Rad}(U) = \{0\}$, donc $\mathrm{Rad}(U^\perp) = U \cap U^\perp = \{0\}$. On obtient d'une part que $U^\perp$ est non dégénéré, et d'autre part une somme directe $U \oplus U^\perp \subset V$. Alors $U \oplus U^\perp = V$ en raison de la dimension. C'est même une somme directe orthogonale car $U$ et $U^\perp$ sont orthogonaux. □

**1.2.3 - Théorème.** *Tout espace quadratique $(V, Q)$ possède une base orthogonale.*

*Démonstration.* Raisonnons par récurrence sur $\dim V$. Si $\dim V = 0$, $V = \{0\}$, le théorème est trivial. Supposons $\dim V \ge 1$. Montrons d'abord qu'on a une décomposition $V = kx \overset{\perp}{\oplus} U$. Si $V$ est non dégénéré et s'il existe $x \in V$ tel que $Q(x) = x \cdot x \neq 0$, alors $kx$ est un sous-espace non dégénéré et donc $V = kx \overset{\perp}{\oplus} U$ avec $U = (kx)^\perp$ (1.2.2, (ii)). Sinon, soit $V$ est dégénéré, soit on a $Q(x) = 0$ pour tout $x \in V$ et on aura $x \cdot y = 0$ pour tous $x, y \in V$ (1.1.1, (ii)) ; dans tous les cas, il existe $x \in \mathrm{Rad}(V)$ non zéro ; en prenant $U$ un supplémentaire de $kx$ dans $V$, on obtient $V = kx \overset{\perp}{\oplus} U$. Ensuite, comme $\dim U = \dim V - 1$, $U$ admet une base orthogonale $\mathscr{E}$ par l'hypothèse de récurrence. Alors $\{x\} \cup \mathscr{E}$ est une base orthogonale de $V$. □

## 1.3 Isotropie

Soit $(V, Q)$ un espace quadratique sur $k$.

**1.3.1.** (i) Un élément $x \in V$ est dit *isotrope* si $Q(x) = 0$. $(V, Q)$ est dit *isotrope* s'il existe un élément isotrope *non zéro* de $V$, *anisotrope* sinon. Autrement dit, $(V, Q)$ est isotrope si $Q$ représente 0, anisotrope sinon. En particulier, un espace anisotrope est non dégénéré, puisque tous les éléments dans $\mathrm{Rad}(V)$ sont isotropes. La propriété d'isotropie est invariante sous isomorphismes d'espaces quadratiques.

(ii) $(V, Q)$ est appelé *plan hyperbolique* s'il a une base $(x, y)$ telle que $Q(x) = Q(y) = 0$ et $x \cdot y \neq 0$. Quitte à diviser $y$ par $x \cdot y$, on peut supposer $x \cdot y = 1$. Donc, tous les plans hyperboliques sont isomorphes l'un aux autres, et en particulier isomorphes à $(k^2, Q_{hyp})$ avec $Q_{hyp} : k^2 \to k, (a, b) \mapsto ab$ ; un plan hyperbolique est non dégénéré.

**1.3.2 - Lemme.** *Supposons $(V, Q)$ non dégénéré. Soient $W \subset V$ un sous-espace vectoriel et $x \in V$ un élément isotrope non zéro tels que l'on a une somme directe orthogonale*

$$W \overset{\perp}{\oplus} kx$$

*Il existe un élément isotrope $y \in V$ tel que $x \cdot y = 1$ et que l'on a une somme directe orthogonale*

$$W \overset{\perp}{\oplus} (kx \oplus ky)$$

*Démonstration.* On a $W^\perp \not\subset (kx)^\perp$ ; sinon on aurait $kx \subset W$ en prenant leurs orthogonaux (1.2.2), absurde. Soit $y_0 \in W^\perp \backslash (kx)^\perp$, alors $y_0 \cdot x \neq 0$, et $y_0 \notin W$ car $W \subset (kx)^\perp$ par l'hypothèse. Il suffit alors de prendre $y = \frac{1}{y_0 \cdot x}\left(y_0 - \frac{y_0 \cdot y_0}{2 y_0 \cdot x} x\right)$. En effet, on vérifie bien que $y \cdot y = 0$, $x \cdot y = 1$, que $y \notin kx$ car $x \cdot x = 0$ mais $y \cdot x \neq 0$, que $y \in W^\perp$ car $y_0, x \in W^\perp$ ; enfin, soit $ax + by \in W$, alors $b = 0$ car $W$ est orthogonal à $x$, et $a = 0$ car $W$ est orthogonal à $y$. Donc on a la somme directe $W \oplus (kx \oplus ky)$ et $kx \oplus ky \subset W^\perp$, d'où la somme directe orthogonale $W \overset{\perp}{\oplus} (kx \oplus ky)$. □

**1.3.3 - Corollaire.** *Si $(V, Q)$ est non dégénéré et isotrope, on a $Q(V) = k$.*

*Démonstration.* Selon (1.3.2) avec $W = 0$ et $x \in V$ isotrope non zéro, il existe $y \in V$ isotrope tel que $x \cdot y = 1$. Alors pour tout $a \in k$, on a $Q(x + \frac{y}{2}) = a$, d'où $Q(V) = k$. □

## 1.4 Théorème de Witt

On s'intéresse à la question du prolongement d'un morphisme métrique *injectif*.

**1.4.1 - Lemme.** *Supposons $(V, Q)$ et $(V', Q')$ espaces quadratiques non dégénérés. Soit $U \subset V$ un sous-espace vectoriel et soit $s : U \to V'$ un morphisme métrique injectif. Si $U$ est dégénéré, on peut prolonger $s$ en un morphisme métrique injectif $s_1 : U_1 \to V'$, où $U_1$ contient $U$ comme hyperplan.*

La démonstration donnée dans [Ser77] (Chap. IV, 1.5, Lemme) est incomplète, parce que son choix de $y'$ ne garantie pas que $s_1$ préserve le produit scalaire entre $y$ et des éléments de $U$ autres que $x$. On la complète à l'aide du lemme 1.3.2.

*Démonstration.* Soit $x \in \mathrm{Rad}(U)$ non zéro ; alors $x \cdot x = 0$, $x$ est un élément isotrope de $V$. Posons $W$ son supplémentaire dans $U$, de sorte que l'on a $U = W \overset{\perp}{\oplus} kx$. Il existe (1.3.2) un $y \in V$ isotrope tel que $x \cdot y = 1$ et que l'on a $W \overset{\perp}{\oplus} (kx \oplus ky)$. D'autre part, comme $s$ est métrique injectif, on a $s(x)$ isotrope et $s(U) = s(W) \overset{\perp}{\oplus} ks(x)$. De même, il existe un $y' \in V'$ isotrope tel que $s(x) \cdot y' = 1$ et que l'on a $s(W) \overset{\perp}{\oplus} (ks(x) \oplus ky')$. Définissons $U_1 := W \overset{\perp}{\oplus} (kx \oplus ky) = U \oplus ky$ et $s_1 : U_1 \to V'$ par $s_1|_U = s, s_1(y) = y'$ ; ils satisfont aux propriétés demandées. □

**1.4.2 - Théorème** (Witt). *Supposons $(V, Q)$ et $(V', Q')$ isomorphes et non dégénérés. Soit $U \subset V$ un sous-espace vectoriel. Tout morphisme métrique injectif $s : U \to V'$ peut être prolongé en un isomorphisme $\tilde{s} : V \xrightarrow{\sim} V'$.*

**1.4.3 - Corollaire.** *Soit $(V, Q)$ un espace quadratique non dégénéré ; soient $U_1, U_2 \subset V$ deux sous-espaces quadratiques isomorphes. Alors $U_1^\perp$ et $U_2^\perp$ sont isomorphes.*

*Démonstration du théorème (1.4.2) et du corollaire (1.4.3).* (a) Observons d'abord que (1.4.2) implique (1.4.3) : il suffit d'appliquer (1.4.2) à $(V, Q) = (V', Q')$ et $s : U_1 \xrightarrow{\sim} U_2 \hookrightarrow V$, et puis prendre les orthogonaux de $U_1$ et de $U_2$.

(b) Démontrons (1.4.2). Comme $(V, Q)$ et $(V', Q')$ sont isomorphes, on peut les supposer identiques ; d'autre part, en utilisant (1.4.1), on peut toujours se ramener au cas où $U$ est *non dégénéré*. Raisonnons alors par récurrence sur $\dim U$ pour tels $U$.

(c) Si $\dim U = 1$, on a $U = kx$ pour un $x \in V$ non isotrope ; posons $y = s(x)$, on a $y \cdot y = x \cdot x$ ; on peut choisir $\varepsilon \in \{\pm 1\}$ tel que $x + \varepsilon y$ ne soit pas isotrope, puisque l'on a

$$(x + y) \cdot (x + y) + (x - y) \cdot (x - y) = 2x \cdot x \neq 0$$

Quitte à remplacer $s$ par $-s$, on peut supposer $x - y$ non isotrope ; alors $k(x - y)$ est un sous-espace de $V$ non dégénéré. Donc (1.2.2, (ii)), $V = k(x-y) \overset{\perp}{\oplus} \big(k(x-y)\big)^\perp$. Soit $\tilde{s} : V \to V$ une symétrie par rapport à $\big(k(x-y)\big)^\perp$, c'est-à-dire

$$\tilde{s} : a(x - y) + z \mapsto -a(x - y) + z \quad \text{où} \quad a \in k, z \in \big(k(x-y)\big)^\perp$$

$\tilde{s}$ est bien un isomorphisme. De plus, comme $(x - y) \cdot (x + y) = x \cdot x - y \cdot y = 0$, on a $x + y \in \big(k(x-y)\big)^\perp$, puis

$$2\tilde{s}(x) = \tilde{s}(x - y) + \tilde{s}(x + y) = -(x - y) + (x + y) = 2y$$

Donc $\tilde{s}(x) = y$, $\tilde{s}|_{kx} = s$. Ainsi, $\tilde{s}$ prolonge $s$.

(d) Si $\dim U > 1$, choisissons un $x \in U$ non isotrope et posons $U_0$ son orthogonal dans $U$ ; donc $U_0$ est *non dégénéré* et on a $U = kx \overset{\perp}{\oplus} U_0$ (1.2.2, (ii)). D'après (c) et (a), on a $(kx)^\perp \simeq \big(ks(x)\big)^\perp$, qui sont d'ailleurs *non dégénérés* (1.2.2, (ii)) ; d'autre part, on a $U_0 \subset (kx)^\perp$, $\dim U_0 < \dim U$ et $s|_{U_0} : U_0 \to \big(ks(x)\big)^\perp$ est un morphisme métrique injectif. Par l'hypothèse de récurrence, on prolonge $s|_{U_0}$ en un isomorphisme $\tilde{s}_0 : (kx)^\perp \xrightarrow{\sim} \big(ks(x)\big)^\perp$. L'application $\tilde{s} : V \to V$ définie par $\tilde{s}|_{kx} = s|_{kx}, \tilde{s}|_{(kx)^\perp} = \tilde{s}_0$ est bien un isomorphisme prolongeant $s$. □

**1.4.4 - Proposition.** *Pour tout espace quadratique $(V, Q)$ non dégénéré, on a*

$$V = U \overset{\perp}{\oplus} mH$$

*où $U$ est un sous-espace anisotrope de $V$, $m \in \mathbb{N}$, $mH$ désigne la somme directe orthogonale de $m$ sous-espaces hyperboliques. L'entier $m$ est unique, et $U$ est unique à isomorphe près.*

*Démonstration.* Comme $0H = \{0\} \subset V$, il existe $m \in N$ tel que $V$ contient un sous-espace $mH$ somme directe orthogonale de $m$ sous-espaces hyperboliques de $V$. Supposons que $m$ soit maximal. Posons $U = (mH)^{\perp}$. Comme $mH$ est non dégénéré, on a $V = U \overset{\perp}{\oplus} mH$ (1.2.2). Si jamais il existe $x \neq 0$ isotrope tel que l'on a $mH \overset{\perp}{\oplus} kx \subset V$, il existe $y \neq 0$ isotrope tel que $y \cdot x = 1$ et $mH \overset{\perp}{\oplus} (kx \oplus ky) \subset V$ (1.3.2). Mais alors $kx \oplus ky$ est hyperbolique, ce qui contredit la maximalité de $m$. Ainsi, $U$ est anisotrope, et on obtient la décomposition $V = U \overset{\perp}{\oplus} mH$.

Pour l'unicité, il suffit d'appliquer (1.4.3) récursivement à un sous-espace hyperbolique s'il en existe un, et de tenir compte du fait que deux espaces quadratiques isomorphes sont soit isotropes, soit anisotropes en même temps (1.3.1, (i)). □

## 1.5 Formes quadratiques usuelles

**1.5.1.** Au sens *usuel*, une forme quadratique à $n$ variables sur $k$ est un polynôme homogène de degré 2 à $n$ variables à coefficients dans $k$. Comme la caractérstique de $k$ n'est pas égale à 2, on peut l'écrire sous la forme

$$f(X) = \sum_{i,j=1}^{n} a_{ij} X_i X_j \quad \text{où} \quad a_{ij} = a_{ji} \in k \tag{1.5.1.1}$$

**1.5.2.** Soit $f$ une forme quadratique usuelle, le couple $(k^n, f)$ est un espace quadratique que l'on peut noter $(V_f, Q_f)$, dit *associé* à $f$. Les définitions et les résultats précédents se transportent sur les formes quadratiques usuelles via $f \rightsquigarrow (V_f, Q_f)$ :

- $f$ est *non dégénérée* si $V_f$ est non dégénéré, on appelle alors $\dim V_f = n$ le *rang* de $f$. Soit $A$ la matrice symétrique telle que $f(X) = {}^tXAX$, alors $f$ est non dégénérée dans ce sens si et seulement si $\det A \neq 0$.
- $f$ et $g$ sont dites *équivalentes* si $V_f \simeq V_g$, et on note alors $f \sim g$. Explicitement, si on écrit $f(X) = {}^tXAX$ et $g(Y) = {}^tYBY$ où $A$ et $B$ sont des matrices symétriques, $f \sim g$ si et seulement s'il existe une matrice inversible $P$ telle que $A = {}^tPBP$.
- Soit $a \in k$. On dit que $f$ *représente* $a$ dans $k$ si $Q_f$ représente $a$, ce qui revient au même de dire que $f = a$ admet une solution non zéro dans $k^n$. Deux formes équivalentes représentent les mêmes éléments dans $k$ (1.1.6).
- La *somme directe* de $f(X_1, \ldots, X_m)$ et $g(X_1, \ldots, X_n)$ $f \dot{+} g$, est la forme quadratique $f(X_1, \ldots, X_m) + g(X_{m+1}, \ldots, X_{m+n})$. On a $V_{f \dot{+} g} \simeq V_f \overset{\perp}{\oplus} V_g$. On pose $f \dot{-} g := f \dot{+} (-g)$.
- On dit que $f$ est *isotrope* si $V_f$ est isotrope (ou également, si elle représente 0), *anisotrope* sinon. Une forme quadratique anisotrope est non dégénérée (1.3.1).
- $f$ est dite *hyperbolique* si $V_f$ est un plan hyperbolique, ou également si $f \sim X_1 X_2$.
- Le *discriminant* de $f$ est défini comme $d(f) := d(Q_f)$. Soit $A$ la matrice symétrique telle que $f(X) = {}^tXAX$, alors $d(f)$ est la classe de $\det A$ dans $k^\times / k^{\times 2} \cup \{0\}$. Si $f$ est non dégénérée, $d(f) \in k^\times / k^{\times 2}$. On a $d(f) = d(g)$ si $f \sim g$.

Comme traductions de (1.2.3), (1.3.3) et (1.4.4), on a les propositions (1.5.3), (1.5.4) et (1.5.7) :

**1.5.3 - Proposition** (Forme diagonale). *Toute forme quadratique est diagonalisable, i.e. équivalente à une forme*

$$a_1X_1^2 + \ldots + a_mX_m^2$$

**1.5.4 - Proposition.** *Si $f$ est non dégénérée et représente 0, il représente tout $a \in k$.*

Cette proposition implique aussitôt les critères de représentabilité suivants :

**1.5.5 - Corollaire.** *Soit $f$ une forme quadratique non dégénérée sur $k$ de rang $n \geq 1$. Soit $a \in k^\times$. Les assertions suivantes sont équivalentes :*

*(i)* $f$ *représente* $a$.

*(ii)* $f \sim h \dot{+} aZ^2$ *où* $h$ *est une forme de rang* $n-1$.

*(iii)* $f \dot{-} aZ^2$ *représente* $0$.

**1.5.6 - Corollaire.** *Soit $g, h$ deux formes quadratiques non dégénérées sur $k$ de rang $\neq 1$. Soit $f = g \dot{-} h$. Les assertions suivantes sont équivalentes :*

*(i)* $f$ *représente 0.*

*(ii) Il existe* $a \in k^\times$ *qui est représenté à la fois par* $g$ *et par* $h$.

*(iii) Il existe* $a \in k^\times$ *tel que* $g \dot{-} aZ^2$ *et* $h \dot{-} aZ^2$ *représentent* $0$ *;*

**1.5.7 - Proposition.** *Si $f$ est non dégénérée, on a*

$$f \sim f_{an} \dot{+} (X_1X_2)^m$$

*où $f_{an}$ est anisotrope, $m \in \mathbb{N}$, et $(X_1X_2)^m$ désigne la somme directe de $m$ copie(s) de $X_1X_2$. De plus, l'entier $m$ est unique; $f_{an}$ est unique à équivalence près. On appelle $m$ l'*indice d'isotropie *de $f$, et $f_{an}$ le* noyau anisotrope *de $f$.*

**1.5.8 (Extension de corps de coefficients).** Soit $f$ une forme quadratique sur $k$ et soit $K/k$ une extension de corps. En identifiant les coefficients de $f$ comme dans $K$ via $k \hookrightarrow K$, on peut voir $f$ comme une forme quadratique sur $K$. Ainsi, $f$ est non dégénérée (*resp.* isotrope, ou représente 0 (1.5.2)) dans $K$ si $f$ l'est dans $k$.

# 2 Nombres $p$-adiques

## 2.1 Définitions et propriétés élémentaires

**2.1.1 (Entiers $p$-adiques).** Pour $n, m \in \mathbb{N}, n \geq m$, on a un morphisme d'anneaux naturel $\varepsilon_{mn} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ donné par la réduction modulo $p^m$. Pour tout $n \in \mathbb{N}$, on munit $\mathbb{Z}/p^n\mathbb{Z}$ de la topologie discrète. $(\mathbb{Z}/p^n\mathbb{Z}, \varepsilon_{mn})$ est un *système projectif d'anneaux topologiques.*

On appelle l'*anneau des entiers $p$-adiques* l'anneau topologique $\mathbb{Z}_p$ défini comme la limite projective de ce système projectif.

On note $\varepsilon_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ les morphismes *continus* définissant cette limite projective. Pour tout anneau topologique $A$ et les morphismes d'anneaux continus $\phi_n : A \to \mathbb{Z}/p^n\mathbb{Z}$ vérifiant $\phi_m = \varepsilon_{mn} \circ \phi_n$ pour $n \geq m$, il existe un unique morphisme d'anneaux continu $\phi : A \to \mathbb{Z}_p$ tel que $\phi_n = \varepsilon_n \circ \phi$. Comme $\varepsilon_n$ sont continus et que $\mathbb{Z}/p^n\mathbb{Z}$ sont discrets, $\ker \varepsilon_n$ sont à la fois *ouverts* et *fermés*, et forment une base de voisinages décroissants de 0. D'ailleurs, la topologie de $\mathbb{Z}_p$ est séparée et on a $\bigcap_n \ker \varepsilon_n = \{0\}$.

**2.1.2 (Injection canonique $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$).** Les morphismes de réduction $\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}, n \in \mathbb{N}$ définissent un morphisme d'anneaux $\iota : \mathbb{Z} \to \mathbb{Z}_p$ (oubliant la topologie) tel que le morphisme composé $\varepsilon_n \circ \iota$ est la réduction modulo $p^n$. Donc $\varepsilon_n \circ \iota$ est surjectif pour tout $n \in \mathbb{N}$. On en déduit que $\iota(\mathbb{Z})$ est *dense* dans $\mathbb{Z}_p$. En effet, d'après (2.1.1), il suffit de montrer que pour tout $n \in \mathbb{N}$, il existe $N \in \mathbb{Z}$ tel que $\iota(N) \in x + \ker \varepsilon_n$ ; pour cela, soit $N$ un entier dont l'image par $\varepsilon_n \circ \iota$ est égale à $\varepsilon_n(x)$, alors $\varepsilon_n \circ \iota(N) = \varepsilon_n(x)$ puis $\varepsilon_n(\iota(N) - x) = 0$, $\iota(N) \in x + \ker \varepsilon_n$.

D'ailleurs, $\iota$ est *injectif* puisque $\ker \iota \subset \bigcap_{n\in\mathbb{N}} \ker(\varepsilon_n \circ \iota) = \bigcap_{n\in\mathbb{N}} p^n\mathbb{Z} = \{0\}$. On peut alors identifier $\mathbb{Z}$ avec $\iota(\mathbb{Z}) \subset \mathbb{Z}_p$.

**2.1.3 ($\varepsilon_k$ est la réduction modulo $p^k$ dans $\mathbb{Z}_p$).** On a $\ker \varepsilon_k = p^k\mathbb{Z}_p$. Ainsi, pour un entier $m \in \mathbb{Z}$, dire que $p$ divise $m \in \mathbb{Z}$ dans $\mathbb{Z}$ équivaut à dire que $p$ divise $m$ dans $\mathbb{Z}_p$. En effet, on a

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\times p^k} & \mathbb{Z} & \xrightarrow{\text{mod } p^k} & \mathbb{Z}/p^k\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & \mathbb{Z}_p & \xrightarrow{\times p^k} & \mathbb{Z}_p & \xrightarrow{\varepsilon_k} & \mathbb{Z}/p^k\mathbb{Z} & \longrightarrow & 0 \end{array} \tag{2.1.3.1}$$

où le diagramme commute et les deux lignes sont des suites exactes courtes.

En effet, pour cela, on a pour tout $n \in \mathbb{N}$ le diagramme commutatif suivant

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\times p^k} & \mathbb{Z} & \xrightarrow{\text{mod } p^k} & \mathbb{Z}/p^k\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \text{mod}} & & \downarrow{\scriptstyle \text{mod}} & & \| & & \\ 0 & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} & \xrightarrow{\times p^k} & \mathbb{Z}/p^{n+k}\mathbb{Z} & \xrightarrow{\text{mod } p^k} & \mathbb{Z}/p^k\mathbb{Z} & \longrightarrow & 0 \end{array}$$

qui est compatible avec les systèmes projectifs $(\mathbb{Z}/p^n\mathbb{Z})_n$ et $(\mathbb{Z}/p^{n+k}\mathbb{Z})_n$, et dont les deux lignes sont des suites exactes courtes. En passant à la limite projective, on obtient le diagramme commutatif (2.1.3.1) avec la seconde ligne *exacte à gauche*, sauf que l'on a $\mathbb{Z}_p \xrightarrow{\varphi} \mathbb{Z}_p$ à la place de $\mathbb{Z}_p \xrightarrow{\times p^k} \mathbb{Z}_p$. Or, ces deux morphismes qui sont *continus* se coïncident sur la partie *dense* (2.1.2) $\mathbb{Z}$ de $\mathbb{Z}_p$ par la commutativité du carré à gauche (2.1.3.1), donc ils sont égaux. De plus, $\varepsilon_n$ est surjectif car $\varepsilon_n \circ \iota$ est surjectif (2.1.2), donc la seconde ligne de (2.1.3.1) est enfin *exacte*.

**2.1.4 (Critère d'inversibilité).** On a $\mathbb{Z}_p \backslash p\mathbb{Z}_p = \mathbb{Z}_p^\times$. Autrement dit, pour $x \in \mathbb{Z}_p$, $p$ ne divise pas $x$ dans $\mathbb{Z}_p$ si et seulement si $x$ est inversible dans $\mathbb{Z}_p$.

En effet, si $x \in \mathbb{Z}_p \backslash p\mathbb{Z}_p$, on a $\varepsilon_1(x) \neq 0$ (2.1.3.1), donc $\varepsilon_1(x) \in (\mathbb{Z}/p\mathbb{Z})^\times$. Comme un entier est inversible dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement s'il est inversible dans $\mathbb{Z}/p^n\mathbb{Z}\,(n \geq 1)$, on a alors $\varepsilon_n(x) \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. On obtient ainsi un *automorphisme* du système projectif $(\mathbb{Z}/p^n\mathbb{Z})_n$ défini par la multiplication par $\varepsilon_n(x)$ sur $\mathbb{Z}/p^n\mathbb{Z}$; sa limite projective, qui est la multiplication par $x$ sur $\mathbb{Z}_p$, est alors un *automorphisme* de $\mathbb{Z}_p$. Donc on a $x \in \mathbb{Z}_p^\times$. Inversement, il est clair que si $x \in \mathbb{Z}_p^\times$, on a $\varepsilon_1(x) \in (\mathbb{Z}/p\mathbb{Z})^\times$, $\varepsilon_1(x) \neq 0$, donc $x \notin p\mathbb{Z}_p$.

**2.1.5 - Proposition.** *On a comme produit direct interne (d'un monoïde et un groupe)*

$$\mathbb{Z}_p \backslash \{0\} = p^{\mathbb{N}} \times \mathbb{Z}_p^\times$$

*plus précisément, tout $x \in \mathbb{Z}_p$ non zéro s'écrit uniquement comme $x = p^n u$ avec $n \in \mathbb{N}$ et $u \in \mathbb{Z}_p$. En particulier, $\mathbb{Z}_p$ est un anneau intègre.*

*Démonstration.* Soit $x \in \mathbb{Z}_p \backslash \{0\}$. Comme $p^0\mathbb{Z}_p = \mathbb{Z}_p$ et que $p^k\mathbb{Z}_p = \ker \varepsilon_k$ (2.1.3.1) décroît avec $k$ ayant $\{0\}$ comme intersection (2.1.1), il existe $k \in \mathbb{N}$ tel que $x = p^k\mathbb{Z}_p \backslash p^{k+1}\mathbb{Z}_p$. Alors il existe $u \in \mathbb{Z}_p$ tel que $x = p^n u$ ; selon notre choix de $k$, on a $u \in \mathbb{Z}_p \backslash p\mathbb{Z}_p$, donc (2.1.4) $u \in \mathbb{Z}_p^\times$.

Montrons l'uncité de cette écriture. Supposons $x = p^k u = p^{k'} u'$ avec $k' \in \mathbb{N}$, $u' \in \mathbb{Z}_p^\times$. On peut supposer $k \leq k'$. Comme la multiplication par $p^k$ sur $\mathbb{Z}_p$ est une application injective (2.1.3.1), on a $u = p^{k'-k}u'$ ; alors $k' - k = 0$ (2.1.4) et puis $u' = u$, d'où l'unicité. Encore par l'injectivité de la multiplication par $p^k$ dans $\mathbb{Z}_p$, on obtient que $p^{\mathbb{N}} = \{p^n : n \in \mathbb{N}\} \simeq (\mathbb{N}, +)$ est un monoïde ne contenant pas 0. Alors $\mathbb{Z}_p \backslash \{0\}$ est un monoïde, produit direct interne du monoïde $p^{\mathbb{N}}$ et le groupe $\mathbb{Z}_p^\times$. En particulier, $\mathbb{Z}_p$ est un anneau intègre. □

**2.1.6 (Nombres $p$-adiques).** Le corps des fractions de $\mathbb{Z}_p$, noté $\mathbb{Q}_p$, est appelé le *corps des nombres $p$-adiques.* On a $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ (2.1.2), donc $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$. Alors $\mathbb{Q}_p$ est *de caractéristique 0.*

**2.1.7 (Structure topologique et métrique sur $\mathbb{Z}_p$ et $\mathbb{Q}_p$).** On a une *valuation $p$-adique* bien définie $v_p : \mathbb{Z}_p \to \mathbb{N} \cup \{+\infty\}$ telle que $v_p(0) = +\infty$ et que $v_p(p^n u) = n$ si $n \in \mathbb{N}$, $u \in \mathbb{Z}_p^\times$.

En vertu de 2.1.5, on a comme produit direct interne (de deux groupes)

$$\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{Z}_p^\times \tag{2.1.7.1}$$

Alors la valuation $v_p$ s'étend sur $\mathbb{Q}_p$ en prenant « l'exposant de $p$ ». La valuation $v_p$ est un morphisme de groupes de $\mathbb{Q}_p^\times$ dans $\mathbb{Z}$, autrement dit, si $x, y \in \mathbb{Q}_p^\times$, on a

$$v_p(xy) = v_p(x) + v_p(y)$$

De plus, $v_p$ vérifie l'inégalité

$$v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$$

On peut définir la distance $d_p(\cdot, \cdot)$ sur $\mathbb{Q}_p$ comme

$$d_p(x, y) = e^{-v_p(x-y)}$$

Muni de la topologie induite par $d_p$, $\mathbb{Q}_p$ est un corp topologique ayant

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : v_p(x) \geq 0\} = \{x \in \mathbb{Q}_p : d_p(x, 0) \leq 1\} = \{x \in \mathbb{Q}_p : d_p(x, 0) < e\}$$

comme un sous-anneau topologique *ouvert* et *fermé.*

Il y a maintenant deux topologies sur $\mathbb{Z}_p$, celle de la limite projective et celle induite de la distance $d_p$ ; il se trouve qu'elles se coïncident. En effet, $(x + p^n\mathbb{Z}_p)_{n\in\mathbb{N}} = (\ker \varepsilon_n)_{n\in\mathbb{N}} = \{y \in \mathbb{Z}_p : v_p(y - x) > n - 1\}$ est une base de voisinages de $x$ dans les deux topologies.

Étant une limite projective d'espaces discrets finis, $\mathbb{Z}_p$ est *compact*, de sorte que l'espace métrique $(\mathbb{Z}_p, d_p)$ est *complet.* $(\mathbb{Q}_p, d_p)$ est alors aussi *complet.* De plus, pour tout $k \in \mathbb{N}$, $p^k\mathbb{Z}_p$ est un *compact* car il est fermé (2.1.1) dans le compact $\mathbb{Z}_p$.

La distance $d_p$ vérifie l'inégalité ultramétrique

$$d_p(x, z) \leq \max\{d_p(x, y), d_p(y, z)\}$$

Par conséquent, une suite $(u_n)$ dans $\mathbb{Z}_p$ (*resp.* dans $\mathbb{Q}_p$) est une suite de Cauchy si et seulement si $\lim_n(u_{n+1} - u_n) = 0$. Par la complétude, une suite $(u_n)$ dans $\mathbb{Z}_p$ (*resp.* dans $\mathbb{Q}_p$) telle que

$\lim_n(u_{n+1}-u_n)=0$ converge dans $\mathbb{Z}_p$ (*resp.* dans $\mathbb{Q}_p$).

**2.1.8.** Si $v_p(x)<v_p(y)$, on a $v_p(x+y)=v_p(x)$. En effet, on a $v_p(x+y)\geq\min\{v_p(x),v_p(y)\}=v_p(x)$, et puis $v_p(x)=v_p(x+y-y)\geq\min\{v_p(x+y),v_p(-y)\}\geq v_p(x)$, d'où $\min\{v_p(x+y),v_p(y)\}=v_p(x)$, d'où $v_p(x+y)=v_p(x)$ car $v_p(y)\neq v_p(x)$.

Par conséquent, si $x,y,z\in\mathbb{Q}_p$ non tous zéros vérifient $v_p(x),v_p(y)\in 2\mathbb{Z}\cup\{+\infty\}$, $v_p(z)\in(2\mathbb{Z}+1)\cup\{+\infty\}$ et $x=y+z$, on a $v_p(x)=v_p(y)<v_p(z)$.

En effet, si $v_p(y)\geq v_p(z)$, on aura soit $z=0$ puis $y=0$, soit $z\neq 0$ puis $v_p(y)>v_p(z)$ en raison de la parité ; alors soit $x=y=z=0$, soit $v_p(x)=v_p(y+z)=v_p(z)$ d'après ce qui précède, ce qui est absurde en raison de la parité.

## 2.2 *Démonstration du Théorème, nécessité, cas dégénéré et cas $n=2$*

*Démonstration du théorème de Hasse-Minkowski (nécessité et cas dégénéré).* Soit $f$ une forme quadratique sur $\mathbb{Q}$. Comme $\mathbb{Q}$ s'injecte dans $\mathbb{Q}_p$ (2.1.6) et dans $\mathbb{R}$, si $f$ représente 0 sur $\mathbb{Q}$, $f$ représente 0 aussi dans $\mathbb{Q}_p$ et dans $\mathbb{R}$ (1.5.8), d'où la nécessité.

D'autre part, si $f$ est dégénérée, $f$ est isotrope et donc représente 0 dans $\mathbb{Q}$ (1.5.2), la suffisance est alors évidente. Par conséquent, dans la suite de la démonstration du théorème de Hasse-Minkowski, on pourra supposer $f$ *non dégénérée.* □

**2.2.1.** Soient $l,p\in\mathbb{N}$ deux nombres premiers distincts, on a $p\nmid l$ dans $\mathbb{Z}$, donc $p\nmid l$ aussi dans $\mathbb{Z}_p$ (2.1.3), alors $l\in\mathbb{Z}_p^\times$ (2.1.4), d'où $v_p(l)=0$ si $l\neq p$. Soit $n\in\mathbb{N}$, on factorise $n=\prod_{p|n}p^{\alpha_p}$ où $p$ sont des premiers distincts ; on obtient alors $\alpha_p=v_p(n)$, donc

$$n=\prod_{p\text{ premier},\,p|n}p^{v_p(n)} \tag{2.2.1.1}$$

*Démonstration du théorème de Hasse-Minkowski (cas $n=2$).* Selon (1.5.3), on a $f\sim X^2-aY^2$ à une constante non zéro près. Montrons la suffisance. Comme $f$ représente 0 dans $\mathbb{R}$, on a $a>0$. Comme $f$ représente 0 dans $\mathbb{Q}_p$, il existe $b\in\mathbb{Q}_p^\times$ tel que $a=b^2$, puis $v_p(a)=2v_p(b)\in 2\mathbb{Z}$. Ainsi, $v_p(a)/2\in\mathbb{Z}$ pour tout $p$ et on obtient (2.2.1.1)

$$a=\prod_{\substack{p\text{ premier}\\ p|a}}p^{v_p(a)}=\left(\prod_{\substack{p\text{ premier}\\ p|a}}p^{v_p(a)/2}\right)^2\in\mathbb{Q}^{\times 2}$$

Donc $f\sim X^2-aY^2\sim X^2-Y^2$ représente 0 dans $\mathbb{Q}$. □

## 2.3 Structure multiplicative de $\mathbb{Z}_p^\times$

**2.3.1 - Proposition** (Relèvement de Teichmüller). *Soient $x\in(\mathbb{Z}/p\mathbb{Z})^\times$ et $\tilde{x}$ un relèvement de $x$ dans $\mathbb{Z}_p$, i.e. tel que $\tilde{x}\equiv x\pmod p$. Alors la suite $(\tilde{x}^{p^n})_{n\in\mathbb{N}}$ a une limite $\tau(x)\in\mathbb{Z}_p^\times$ qui ne dépend pas du choix de $\tilde{x}$, et qui vérifie $\tau(x)^p=\tau(x)$ et $\tau(x)\equiv x\pmod p$. On appelle $\tau(x)$ le* relèvement de Teichmüller *de $x$.*

En fait, on peut aussi définir $\tau(x)$ pour $x=0\in\mathbb{Z}/p\mathbb{Z}$ ; dans ce cas, pour tout relèvement $\tilde{x}$ de 0, il existe $x_1\in\mathbb{Z}_p$ tel que $\tilde{x}=px_1$, alors $\tilde{x}^m=p^mx_1^m$ tend vers $0\in\mathbb{Z}_p$ lorsque $m\to\infty$. Cependant, on se contentera du cas $x\in(\mathbb{Z}/p\mathbb{Z})^\times$.

*Démonstration.* Prouvons l'unicité. Soient $\tilde{x}, \tilde{y} \in \mathbb{Z}_p$ relevant le même $x \in (\mathbb{Z}/p\mathbb{Z})^\times$. On a

$$\tilde{y}^{p^{n+1}} - \tilde{x}^{p^{n+1}} = (\tilde{y}^{p^n} - \tilde{x}^{p^n}) \left[ \sum_{i=0}^{p-1} (\tilde{y}^{p^n})^i (\tilde{x}^{p^n})^{p-1-i} \right] \tag{2.3.1.1}$$

$$\text{où } \left[ \cdots \right] \equiv \sum_{i=0}^{p-1} (x^{p^n})^i (x^{p^n})^{p-1-i} \equiv p(x^{p^n})^{p-1} \equiv 0 \pmod{p} \tag{2.3.1.2}$$

pour tout $n \in \mathbb{N}$. Donc la suite $\left( v_p(\tilde{y}^{p^n} - \tilde{x}^{p^n}) \right)_{n \in \mathbb{N}}$ est strictement croissante, puis

$$\lim_n (\tilde{y}^{p^n} - \tilde{x}^{p^n}) = 0$$

d'où l'unicité.

Prouvons ensuite l'existence de la limite. Si $\tilde{x}$ relève $x$, alors $\tilde{x}^p \equiv x^p \equiv x \pmod{p}$ d'après Fermat, donc $\tilde{x}^p$ relève aussi $x$. En posant $\tilde{y} = \tilde{x}^p$ dans la limite ci-dessus, on obtient

$$\lim_n (\tilde{x}^{p^{n+1}} - \tilde{x}^{p^n}) = 0$$

d'où l'existence de la limite par (2.1.7). Le reste en découle aussitôt. □

**2.3.2 - Corollaire.** *On a une injection de groupes $\tau : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$. Son image, notée $U_{p-1}$, est cyclique d'ordre $p-1$. on a comme produit direct interne*

$$\mathbb{Z}_p^\times = U_{p-1} \times (1 + p\mathbb{Z}_p)$$

*De plus, on a*

$$U_{p-1} = \{x \in \mathbb{Z}_p : x^{p-1} = 1\}$$

*Démonstration.* Il résulte aussitôt de l'unicité de la limite que $\tau$ est un morphisme de groupes. Comme $\tau(x) \equiv x \pmod{p}$, $\tau$ est injectif, $U_{p-1} \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$, et la suite exacte courte

$$1 \to 1 + p\mathbb{Z}_p \longrightarrow \mathbb{Z}_p^\times \xrightarrow{\bmod p} (\mathbb{Z}/p\mathbb{Z})^\times \to 1$$

est scindée, d'où la décomposition comme produit direct interne.

Pour le dernier point, on a $U_{p-1} \subset \{x \in \mathbb{Z}_p : x^{p-1} = 1\}$ puisque $U_{p-1}$ est l'image d'un groupe de cardinal $p-1$ et d'après Lagrange ; d'autre part, l'équation $x^{p-1} = 1$ de $x$ admet *au plus* $p-1$ racines dans le *corps* $\mathbb{Q}_p$, donc l'ensemble de ses racines dans $\mathbb{Z}_p$ ne peut contenir plus d'éléments que $U_{p-1}$. □

*2.3.3 - Remarque.* Dans le cas $p = 2$, $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$, et la décomposition $\mathbb{Z}_2^\times = \{1\} \times (1 + 2\mathbb{Z}_2)$ est triviale ; d'ailleurs, on a comme produit direct interne

$$\mathbb{Z}_2^\times = \{\pm 1\} \times (1 + 4\mathbb{Z}_2)$$

En effet, la suite exacte courte $1 \to 1 + 4\mathbb{Z}_2 \to \mathbb{Z}_2^\times \xrightarrow{\bmod 4} (\mathbb{Z}/4\mathbb{Z})^\times \to 1$ est scindée par la section $(\mathbb{Z}/4\mathbb{Z})^\times \to \{\pm 1\}$, $\overline{\pm 1} \mapsto \pm 1$.

Grâce à ces décompositions en produit direct interne, on se ramène à étudier $1 + p^k\mathbb{Z}_p$.

## 2.4 Structure multiplicative de $1+p^k\mathbb{Z}_p$

Pour tout $k \in \mathbb{N}^*$, munis de la topologie induite de celle de $\mathbb{Z}_p$, $1+p^k\mathbb{Z}_p$ et $p^k\mathbb{Z}_p$ sont des groupes topologiques *séparés* et *compacts* (2.1.7), respectivement multiplicatif et additif.

**2.4.1 - Proposition.** *Soit $p$ un nombre premier; soit $k \geq 1$ si $p \neq 2$, $k \geq 2$ si $p = 2$. Pour tout $x \in 1+p^k\mathbb{Z}_p$, l'application suivante (due à [Lub]), appelée le* logarithme,

$$\log : \ 1+p^k\mathbb{Z}_p \to p^k\mathbb{Z}_p, \quad y \mapsto \lim_{n\to\infty} \frac{y^{p^n}-1}{p^n} \tag{2.4.1.1}$$

*est bien définie et est un isomorphisme de groupes topologiques.*

*Démonstration.* D'abord, le logarithme est bien défini et on a (voir la démontration en bas)

$$v_p\big(\log(1+p^k x)\big) = v_p(p^k x) \tag{2.4.1.2}$$

Nous allons montrer que le logarithme est un morphisme de groupes qui est d'ailleurs continu, fermé et bijectif, il sera alors un isomorphisme de groupes topologiques.

D'abord, le logarithme est un *morphisme de groupes*; en effet, comme tout $y \in 1+p^k\mathbb{Z}_p$ est un relèvement de $1 \in \mathbb{Z}/p\mathbb{Z}$, on a (2.3.1) $\lim_n y^{p^n} = 1$; donc, pour $y', y \in 1+p^k\mathbb{Z}_p$

$$\log(y'y) = \lim_n \frac{(y'y)^{p^n}-1}{p^n} = \lim_n \left(\frac{y'^{p^n}-1}{p^n} y^{p^n} + \frac{y^{p^n}-1}{p^n}\right) = \log y' + \log y$$

Ce morphisme de groupes est *injectif* puisque $\log(1+p^k x) = 0$ implique (2.4.1.2) $p^k x = 0$, puis $x = 0$ car $\mathbb{Z}_p$ est un anneau intègre (2.1.5). $\log(y)$ est continu en $y = 1$ par (2.4.1.2), donc est aussi *continue* en tout $y \in 1+p^k\mathbb{Z}_p$. Comme $1+p^k\mathbb{Z}_p$ est compact et que $p^k\mathbb{Z}_p$ est séparé, $\log(\cdot)$ est une application *fermée.*

Montrons que $\log(\cdot)$ est *surjectif.* Remarquons que $\log\left(1+p^k\mathbb{Z}_p\right) \supset \mathbb{Z}\log(1+p^k)$, que l'adhérence de $\mathbb{Z}\log(1+p^k)$ est $\mathbb{Z}_p\log(1+p^k)$, et enfin que $v_p\big(\log(1+p^k)\big) = v_p(p^k)$ (2.4.1.2). On en conclut que l'adhérence de $\log\left(1+p^k\mathbb{Z}_p\right)$ dans $p^k\mathbb{Z}_p$ contient

$$\mathbb{Z}_p \log(1+p^k) = \mathbb{Z}_p \cdot p^k = p^k\mathbb{Z}_p$$

Comme $\log(\cdot)$ est fermé, on a $\log\left(1+p^k\mathbb{Z}_p\right) = p^k\mathbb{Z}_p$. □

*2.4.2 - Remarque.* Cette définition (2.4.1.1) du logarithme sur $\mathbb{Q}_p$ est un analogue de la formule de l'analyse sur $\mathbb{R}$

$$\log x = \lim_{n\to\infty} n(x^{1/n}-1)$$

Quand $n \to \infty$, on a $\frac{1}{n} \to 0$ dans $\mathbb{R}$ alors que $p^n \to 0$ dans $\mathbb{Q}_p$. De plus, la définition (2.4.1.1) coïncide avec la définition plus usuelle (notée ici avec un tilde) $\widetilde{\log} y := \sum_{n=1}^{\infty}(-1)^n(y-1)^n/n$; en effet, on peut montrer que $y = \exp\left(\widetilde{\log} y\right)$ et puis que

$$\lim_{n\to\infty} \frac{y^{p^n}-1}{p^n} = \lim_{n\to\infty} \frac{\left(\exp\left(\widetilde{\log} y\right)\right)^{p^n}-1}{p^n} = \lim_{n\to\infty} \frac{\exp\left(p^n\widetilde{\log} y\right)-1}{p^n} = \widetilde{\log} y$$

*Démonstration de ce que* $\log(\cdot)$ *est bien défini et de (2.4.1.2).* Pour tout $n \in \mathbb{N}, x \in \mathbb{Z}_p$, posons

$$\varphi_n(x) = (1+p^k x)^{p^n} - 1, \quad \eta_n(x) = p^{-n}\varphi_n(x)$$

Il faut montrer que $\log\Big(1+p^k x\Big) := \lim_{n\to\infty} \eta_n(x)$ est bien défini et que $v_p\Big(\log\Big(1+p^k x\Big)\Big) = v_p(p^k x)$.

On a pour tout $n \geq 1$

$$(1+p^k x)^{p^{n+1}} - 1 = \Big((1+p^k x)^{p^n} - 1\Big) \sum_{i=0}^{p-1} \Big((1+p^k x)^{p^n}\Big)^i$$

$$\varphi_{n+1}(x) = \varphi_n(x) \sum_{i=0}^{p-1} (1+\varphi_n(x))^i = \varphi_n(x)\Big(p + \varphi_n(x)R(\varphi_n(x))\Big)$$

où $R \in \mathbb{Z}_p[X]$ est un polynôme tel que $\sum_{i=0}^{p-1}(1+X)^i = p + XR(X)$. Le coefficient constant de $R$ est égal à $\sum_{i=0}^{p-1} i$. En divisant l'égalité ci-dessus par $p^{n+1}$, on obtient

$$\eta_{n+1}(x) = \eta_n(x)\Big(1 + \frac{\varphi_n(x)}{p} R(\varphi_n(x))\Big)$$

D'une part, $1+p^k x$ et 1 étant deux relèvements de $1 \in \mathbb{Z}/p\mathbb{Z}$, la suite $\big(v_p(\varphi_n(x))\big)_n$ est strictement croissante par (2.3.1.1) et (2.3.1.2), donc $v_p(\varphi_n(x)/p)$ croît avec $n$ et tend vers l'infini ; par conséquent, $\lim_{n\to\infty}(\eta_{n+1}(x) - \eta_n(x)) = 0$, donc (2.1.7) $\lim_{n\to\infty} \eta_n(x)$ existe, le logarithme (2.4.1.1) est bien défini.

D'autre part, Pour tout $n \in \mathbb{N}$, on a par ce qui précède $v_p(\varphi_n(x)/p) \geq v_p(\varphi_0(x)/p) = v_p(p^{k-1}x) \geq k-1$. Donc $v_p(\varphi_n(x)/p) \geq 1$ pour $n \geq 0$ si $p = 2$, et pour $n \geq 1$ si $p \neq 2$. De plus, dans le cas $p \neq 2$, $p$ est impair, le coefficient constant de $R$ est égal à $\sum_{i=0}^{p-1} i = \frac{p-1}{2}p$ ; comme $k \geq 1$, on a alors $R(\varphi_0(x)) = R(p^k x) \in \frac{p-1}{2}p + (p^k x)\mathbb{Z}_p \subset p\mathbb{Z}_p$. On en conclut que pour tout $n \in \mathbb{N}$

$$\frac{\varphi_n(x)}{p} R(\varphi_n(x)) \in p\mathbb{Z}_p$$

d'où

$$v_p\Big(\frac{\eta_{n+1}(x)}{\eta_n(x)}\Big) = v_p\Big(1 + \frac{\varphi_n(x)}{p} R(\varphi_n(x))\Big) = 0$$

On a donc $v_p(\eta_{n+1}(x)) = v_p(\eta_n(x))$ pour tout $n \in \mathbb{N}$, et alors

$$v_p\Big(\log\Big(1+p^k x\Big)\Big) = \lim_n v_p(\eta_n(x)) = v_p(\eta_0(x)) = v_p\Big(\frac{(1+p^k x)-1}{1}\Big) = v_p(p^k x)$$

Ainsi, on a démontré l'identité (2.4.1.2). □

**2.4.3 - Corollaire.** *On a des isomorphismes de groupes topologiques :*

$$1 + p\mathbb{Z}_p \overset{\log}{\simeq} p\mathbb{Z}_p \quad \textit{si } p \neq 2$$
$$1 + 4\mathbb{Z}_p \overset{\log}{\simeq} 4\mathbb{Z}_2 \quad \textit{si } p = 2$$
$$1 + 8\mathbb{Z}_p \overset{\log}{\simeq} 8\mathbb{Z}_2 \quad \textit{si } p = 2$$

*En particulier, si* $p \neq 2$, $1 + p\mathbb{Z}_p$ *est sans torsion et* $1 + p\mathbb{Z}_p = (1 + p\mathbb{Z}_p)^2$ *; si* $p = 2$, $1 + 4\mathbb{Z}_2$ *est sans torsion et* $1 + 8\mathbb{Z}_2 = (1 + 4\mathbb{Z}_2)^2$.

*Démonstration.* Les isomorphes résultent aussitôt de la proposition. De plus, si $p \neq 2$, on a $p \nmid 2$, puis (2.1.4) $2 \in \mathbb{Z}_p^\times$ et donc $2p\mathbb{Z}_p = p\mathbb{Z}_p$. Alors les assertions finales s'ensuivent, compte tenu des isomorphismes. □

**2.4.4 - Corollaire.** *(i) On a comme produit direct interne*

$$\begin{aligned}
\mathbb{Q}_p^\times &= p^{\mathbb{Z}} \times U_{p-1} \times (1 + p\mathbb{Z}_p) \quad \textit{si } p \neq 2 \\
\mathbb{Q}_p^{\times 2} &= p^{2\mathbb{Z}} \times U_{p-1}^2 \times (1 + p\mathbb{Z}_p) \quad \textit{si } p \neq 2 \\
\mathbb{Q}_2^\times &= 2^{\mathbb{Z}} \times \{\pm 1\} \times (1 + 4\mathbb{Z}_2) \quad \textit{si } p = 2 \\
\mathbb{Q}_2^{\times 2} &= 2^{2\mathbb{Z}} \times \{1\} \times (1 + 8\mathbb{Z}_2) \quad \textit{si } p = 2
\end{aligned}$$

*Ces décompositions sont compatibles avec les inclusions $\mathbb{Q}_p^{\times 2} \subset \mathbb{Q}_p^\times$ et celles des composantes.*

*(ii) Étant considéré comme $\mathbf{F}_2$-espace vectoriel, $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ admet une base $\{\overline{u}, \overline{p}\}$ si $p \neq 2$ où $u \in \mathbb{Z}_p^\times$ est un non carré* mod $p$*, et $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ admet une base $\{\overline{2}, \overline{-1}, \overline{5}\}$. On a $\left|\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}\right| = 4$ si $p \neq 2$ et $\left|\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}\right| = 8$.*

*(iii) L'ensemble des racines de l'unité de $\mathbb{Q}_p^\times$ est $U_{p-1}$ si $p \neq 2$, $\{\pm 1\}$ si $p = 2$.*

*(iv) $\mathbb{Q}_p^{\times 2}$ est un ouvert dans $\mathbb{Q}_p$ ; donc $\mathbb{Q}_p^{\times 2}$ est un sous-groupe ouvert de $\mathbb{Q}_p^\times$.*

*Démonstration.* (i) et (ii) découlent aussitôt de (2.1.7.1), (2.3.2), (2.3.3) et (2.4.3). (iii) découle de (i), compte tenu du fait que $p^{\mathbb{Z}} \simeq \mathbb{Z}$ et $1 + p^k\mathbb{Z}_p \simeq p^k\mathbb{Z}_p$ sont sans torsion. Pour (iv), il suffit de remarquer que selon (i), $\mathbb{Q}_p^{\times 2}$ est un sous-groupe de $\mathbb{Q}_p^\times$ contenant l'ouvert $1 + p^3\mathbb{Z}_p \subset \mathbb{Q}_p$. □

**2.4.5 (Places et $\mathbb{Q}_\infty$).** Définissons l'ensemble des *places* de $\mathbb{Q}$ comme

$$V := \{\infty\} \cup \{p \in \mathbb{N} : p \text{ nombre premier}\}$$

Posons $\mathbb{Q}_v := \mathbb{Q}_p$ si $v = p$ est un nombre premier, et $\mathbb{Q}_\infty := \mathbb{R}$ avec la topologie usuelle. On a étudié $\mathbb{Q}_p$ dans les numéros précédents. Pour $\mathbb{Q}_\infty$, on a des propriétés correpondantes :

$\mathbb{Q}_\infty$ est un corps topologique. $\mathbb{Q}$ s'injecte naturellement dans $\mathbb{Q}_\infty$. $\mathbb{Q}_\infty^{\times 2}$ est un ouvert dans $\mathbb{Q}_\infty$ et un sous-groupe ouvert de $\mathbb{Q}_\infty^\times$ d'indice 2. Le groupe quotient $\mathbb{Q}_\infty^\times/\mathbb{Q}_\infty^{\times 2}$ a deux éléments ; il peut être regardé comme un $\mathbf{F}_2$-espace vectoriel dont la base est $\{\overline{a}\}$ où $a < 0$.

On peut alors reformuler le théorème de Hasse-Minkowski comme suivant :

**Théorème** (Hasse-Minkowski). *Une forme quadratique sur $\mathbb{Q}$ représente 0 dans $\mathbb{Q}$ si et seulement si elle représente 0 dans $\mathbb{Q}_v$ pour tout $v \in V$.*

## 2.5 Lemme de Hensel

**2.5.1 - Lemme** (Hensel). *Soit $f \in \mathbb{Z}_p[X]$ et notons $f'$ sa dérivée. Soient $x \in \mathbb{Z}_p, n, k \in \mathbb{Z}$ tels que $0 \leq 2k < n$. Supposons que*

$$\begin{aligned}
v_p(f(x)) &\geq n \\
v_p(f'(x)) &= k
\end{aligned}$$

*Alors, il existe $y \in \mathbb{Z}_p$ tel que*

$$\begin{aligned} v_p(y-x) &\geq n-k \\ v_p(f(y)) &\geq n+1 \\ v_p(f'(y)) &= k \end{aligned}$$

*Démonstration.* On désigne un terme de $p$-valuation plus grande que $s$ par $O(p^s)$. Posons $y = x - \frac{f(x)}{f'(x)}$. Alors on a $y - x = O(p^{n-k})$ par l'hypothèse, puis $y \in \mathbb{Z}_p$, $f(y) = f(x) + f'(x)(y-x) + O(p^{2(n-k)}) = 0 + O(p^{n+n-2k}) = O(p^{n+1})$ et $f'(y) = f'(x) + O(p^{n-k}) = f'(x) + O(p^{k+1})$. □

**2.5.2 - Théorème.** *Soit $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$ et notons $\partial_j f$ ses dérivées partielles. Soient $x = (x_i) \in \mathbb{Z}_p^m$, $n, k \in \mathbb{Z}$ tels que $0 \leq 2k < n$. Supposons que*

$$\begin{aligned} v_p(f(x)) &\geq n \\ v_p(\partial_j f(x)) &= k \end{aligned}$$

*pour un $j \in \{1, \ldots, m\}$. Alors, il existe $y \in \mathbb{Z}_p^m$ tel que*

$$\begin{aligned} v_p(y-x) &\geq n-k \\ f(y) &= 0 \end{aligned}$$

*de plus, on peut demander que $y_i = x_i$ pour tout $i \neq j$.*

*Idée de la démonstration.* Si $m = 1$, on peut appliquer le lemme de Hensel inductivement et obtenir une suite $(y_n)_n$ telle que $v_p(y_n - x) \to \infty$ et $f(y_n) \to 0$. La limite $y = \lim_n y_n$ satisfait aux conditions. Si $m > 1$, et soit $j$ comme dans l'énoncé, on peut regarder $x_i$ $(i \neq j)$ comme des paramètres fixés et appliquer le cas $m = 1$ à $f(x_1, \ldots, X_i, \ldots, x_m) \in \mathbb{Z}_p[X_i]$. □

Ce théorème sera important pour réduire l'existence de solution dans $\mathbb{Z}_p$ à celle modulo un certain $p^n$. En particulier, si $f$ est un polynôme homogène de degré 2 diagonalisé, notant que la dérivé partielle $\partial_j$ vont produire un facteur 2 qui n'est inversible dans $\mathbb{Z}_p$ que pour $p \neq 2$, on a besoin de distinguer les deux cas :

**2.5.3 - Corollaire** ($p \neq 2$). *Supposons $p \neq 2$. Soit $c \in \mathbb{Z}_p$.*

*(i) Soit $f(X) = a_1 X_1^2 + \ldots + a_m X_m^2$ une forme quadratique à coefficients dans $\mathbb{Z}_p^\times$. Toute solution non zéro de $f(x) = c$ dans $(\mathbb{Z}/p\mathbb{Z})^m$ se relève en une solution non zéro dans $\mathbb{Z}_p^m$.*

*(ii) Si de plus $m \geq 3$, $f(x) = c$ admet une solution non zéro dans $\mathbb{Z}_p^m$.*

*Démonstration.* (i) Notons que toute solution non zéro de $f(x) = c$ dans $(\mathbb{Z}/pZ)^m$ $(p \neq 2)$ est représenté par un $x \in \mathbb{Z}_p^m$ non zéro tel que $v_p(f(x) - c) \geq 1$ et $v_p(\partial_j(f(x) - c)) = 0$ pour un $j$ entre 1 et $m$. On peut alors appliquer le théorème avec $n = 1$, $k = 0$ et obtenir une solution dans $\mathbb{Z}_p^m$ congrue à $x$ modulo $p$, donc non zéro. (ii) en découle, compte tenu du fait que toute forme quadratique non dégénérée de rang $m \geq 3$ admet une solution non zéro dans $(\mathbb{Z}/p\mathbb{Z})^m$ [Ser77, Chap. I, n° 2.2, Cor. 2]. □

*2.5.4 - Exemple* ($p \neq 2$). Soit $c \in \mathbb{Z}_p^\times$, alors $c$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $c \in \mathbb{Q}_p^{\times 2}$.

En effet, on a $c \not\equiv 0 \pmod{p}$ selon la condition et (2.1.4), la nécessité résulte du corollaire appliqué à l'équation $x^2 = c$ ; inversement, si $c = a^2$ avec $a \in \mathbb{Q}_p^\times$, on a $v_p(a) = v_p(c)/2 \geq 0$, donc $a \in \mathbb{Z}_p$ (2.1.7), alors $c \equiv a^2 \pmod{p}$ est un carré.

*2.5.5 - Exemple* ($p \neq 2$). Soient $a, b \in \mathbb{Z}$ avec $v_p(a) = 0$, $v_p(b) = 1$. $z^2 - ax^2 - by^2 = 0$ représente 0 dans $\mathbb{Q}_p \Leftrightarrow \left(\frac{a}{p}\right) = 1$. En particulier, $z^2 + x^2 - py^2 = 0$ représente 0 dans $\mathbb{Q}_p \Leftrightarrow \left(\frac{-1}{p}\right) = 1$.

En effet, si $\left(\frac{a}{p}\right) = 1$, $z^2 - a = 0$ a une solution dans $\mathbb{Q}_p$ selon l'exemple précédent ; inversement, si $z^2 - ax^2 - by^2 = 0$ a une solution non zéro dans $\mathbb{Q}_p^3$, on a $2v_p(z) = 2v_p(x) < 1 + 2v_p(y)$ puis $x \neq 0$ et $v_p(z) = v_p(x) \leq v_p(y)$ en appliquant (2.1.8) à l'équation $z^2 = ax^2 + by^2$, donc $z/x \in \mathbb{Z}_p$ et $(z/x)^2 = a \pmod{p}$.

**2.5.6 - Corollaire** ($p = 2$). *Soient $c \in \mathbb{Z}_2$ et $f(X) = a_1X_1^2 + \ldots + a_nX_n^2$ une forme quadratique à coefficients dans $\mathbb{Z}_2$. Toute solution de $f(x) = c$ dans $\mathbb{Z}_2/8\mathbb{Z}_2 \simeq \mathbb{Z}/8\mathbb{Z}$ telle que tout $2a_ix_i$ ne s'annule pas dans $\mathbb{Z}_2/4\mathbb{Z}_2 = \mathbb{Z}/4\mathbb{Z}$, ou ce qui revient au même de dire que tout $a_ix_i$ ne s'annule pas dans $\mathbb{Z}_2/2\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$, se relève en une solution dans $\mathbb{Z}_2$.*

*2.5.7 - Exemple* ($p = 2$). $z^2 + 2x^2 - 5y^2 = 0$ n'a aucune solution non zéro dans $\mathbb{Q}_2^3$ ; mais $z^2 + 2x^2 + 5y^2 = 0$ en a au moins une.

En effet, pour la première équation, supposons $(x, y, z) \neq (0, 0, 0)$ une solution de $z^2 + 2x^2 - 5y^2 = 0$ dans $\mathbb{Q}_2^3$ ; en appliquant (2.1.8) à l'équation $z^2 = 5y^2 - 2x^2$, on obtient $v_2(z) = v_2(y) \leq v_2(x)$ et $z \neq 0$, donc $x/z, y/z \in \mathbb{Z}_2$ et ils vérifient $1 + 2(x/z)^2 - 5(y/z)^2 = 0$ ; mais cette équation n'a pas de solution modulo 8, absurde.

Pour la deuxième équation, l'équation $2x^2 + 5y^2 = -1 \pmod 8$ a une solution non zéro $(x, y) = (1, 1)$ vérifiant $2 \cdot 5y \equiv 2 \cdot 5 \cdot 1 \equiv 2 \not\equiv 0 \pmod 4$, le corollaire s'applique donc à $f = 2x^2 + 5y^2$ et $c = -1$, et nous donne une solution de $1 + 2x^2 + 5y^2 = 0$ dans $\mathbb{Z}_2^2$.

## 2.6 Théorème d'approximation

Dans ce numéro, on pose $S$ une partie *finie* de $V$.

On a une application *injective* $\mathbb{Q} \to \prod_{v \in S} \mathbb{Q}_v$, $x \mapsto (x_v)_{v \in S}$ où $x_v$ est l'image de $x$ via $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$. On peut ainsi voir $\mathbb{Q}$ comme inclus dans $\prod_{v \in S} \mathbb{Q}_v$. On a le théorème suivant [Ser77, Chap. III, n° 2.2, Lmm. 2] :

**2.6.1 - Théorème** (Théorème d'approximation). *$\mathbb{Q}$ est dense dans $\prod_{v \in S} \mathbb{Q}_v$.*

**2.6.2 - Corollaire.** *Soit $f \in \mathbb{Q}[X_1, \ldots, X_n]$ un polynôme. Soient $x_{1,v}, \ldots, x_{n,v}, c_v \in \mathbb{Q}_v$ pour $v \in S$ tels que $f(x_{1,v}, \ldots, x_{n,v}) = c_v \neq 0$. Il existe $x_1, \ldots, x_n \in \mathbb{Q}$ tels que $f(x_1, \ldots, x_n) \in c_v\mathbb{Q}_v^{\times 2}$ pour tout $v \in S$.*

*Démonstration.* $\mathbb{Q}_v$ étant un corps topologique pour tout $v \in V$, tous les polynômes là-dessus sont des fonctions continues, et en particulier pour $f$ vu comme un polynôme sur $\mathbb{Q}_v$. Par conséquent, quand $x_i \in \mathbb{Q}$ rapproche $(x_{i,v})_{v,S}$ dans $\prod_{v \in S} \mathbb{Q}_v$ (ce qui est possible selon le théorème), $f(x_1, \ldots, x_n)$ rapproche $\left(f(x_{1,v}, \ldots, x_{n,v})\right)_{v \in S} = (c_v)_{v \in S}$ dans $\prod_{v \in S} \mathbb{Q}_v$. Comme $c_v \neq 0$ et que $\mathbb{Q}_v^{\times 2}$ est ouvert (2.4.4, (iv)) (2.4.5), $c_v\mathbb{Q}_v^{\times 2}$ est un voisinage ouvert de $c_v$ dans $\mathbb{Q}_v$. Il existe donc $x_1, \ldots, x_n \in \mathbb{Q}$ tels que $f(x_1, \ldots, x_n) \in c_v\mathbb{Q}_v^{\times 2}$ pour tout $v \in S$. □

## 2.7 *Démonstration du Théorème, cas $n \geq 5$, réduction au cas $n = 4$*

*Démonstration du théorème de Hasse-Minkowski (cas $n \geq 5$).* On veut montrer par récurrence que les cas $n \geq 5$ pourront se réduire au cas $n = 4$. Pour cela, soit $n \geq 5$, et montrons que si le théorème est vrai pour les formes de rang $n - 1$, il est aussi vrai pour celles de rang $n$.

Soit $f$ une forme quadratique non dégénérée de rang $n$ sur $\mathbb{Q}$. $f$ étant diagonalisable (1.5.3), on peut écrire $f \sim g \dot{-} h$, où $g$ est non dégénérée de rang 2 et $h$ est de la forme

$$h = a_3 X_3^2 + \ldots + a_n X_n^2$$

avec $a_i \in \mathbb{Q}^\times$. $h$ est de rang $n - 2 \geq 3$. Posons alors

$$S = \{v \in V : a_i \notin \mathbb{Z}_v^\times \text{ pour tout } i \geq 3\} \cup \{\infty, 2\}$$

C'est une partie *finie* de $V$ compte tenu de (2.2.1). Procédons alors en trois étapes :

(i) Il existe $c \in \mathbb{Q}^\times$ représenté par $g$ dans $\mathbb{Q}$ et dans tout $\mathbb{Q}_v$, et par $h$ dans $\mathbb{Q}_v$ pour $v \in S$.

En effet, par l'hypothèse et selon (1.5.6), il existe pour tout $v \in V$ un $c_v \in \mathbb{Q}_v^\times$ représenté à la fois par $g$ et par $h$ dans $\mathbb{Q}_v$, par exemple, il existe $x_{1,v}, x_{2,v} \in \mathbb{Q}_v$ tels que

$$g(x_{1,v}, x_{2,v}) = c_v$$

$S$ étant fini, en vertu de (2.6.2), on peut trouver $x_1, x_2 \in \mathbb{Q}$ tels que $g(x_1, x_2) \in c_v \mathbb{Q}_v^{\times 2}$ pour tout $v \in S$. On a $g(x_1, x_2) \in \mathbb{Q}^\times$ car $c_v \neq 0$. Posons

$$c := g(x_1, x_2)$$

Alors il est clair que $g$ représente $c$ dans $\mathbb{Q}$ et dans tout $\mathbb{Q}_v$. De plus, comme $c \in c_v \mathbb{Q}_v^{\times 2}$ et que $h$ est une forme *quadratique* représentant $c_v$ dans $\mathbb{Q}_v$, $h$ représente aussi $c$ dans $\mathbb{Q}_v$.

(ii) $h$ représente 0 dans $\mathbb{Q}_v$ pour $v \notin S$. En effet, si $v \notin S$, on a $v = p \neq 2$ et $a_i \in \mathbb{Z}_v^\times$ pour $i \geq 3$ selon le choix de $S$, donc $h$ représente 0 dans $\mathbb{Q}_v$ puisque $h$ est de rang $\geq 3$ (2.5.3, (ii)).

(iii) Appliquons l'hypothèse de réccurrence à la forme quadratique

$$cZ^2 \dot{-} h \tag{2.7.0.1}$$

qui est non dégénérée de rang $n - 1$ et qui représente 0 dans tout $\mathbb{Q}_v$ selon (i) et (ii). Alors, $cZ^2 \dot{-} h$ représente 0 dans $\mathbb{Q}$ par l'hypothèse de récurrence, donc $h$ représente $c$ dans $\mathbb{Q}$ (1.5.5). Mais $c$ est aussi représenté par $g$ dans $\mathbb{Q}$, donc (1.5.6) $f = g \dot{-} h$ représente 0 dans $\mathbb{Q}$. □

# 3 Symbole de Hilbert

Soit $k = \mathbb{Q}$ ou $k = \mathbb{Q}_v$ pour $v \in V$. Alors $k$ est un corps de caractéristique $0 \neq 2$.

## 3.1 Définition et une caractérisation

**3.1.1 - Définition** (symbole de Hilbert). Soient $a, b \in k^\times$. Posons

$$\begin{aligned} (a,b)_k &= 1 \quad \text{si } z^2 - ax^2 - by^2 = 0 \text{ admet une solution non zéro dans } k^3 \\ (a,b)_k &= -1 \quad \text{sinon} \end{aligned}$$

On appelle $(a, b)_k$ le *symbole de Hilbert* de $a$ et $b$, relativement à $k$. On peut le simplement noter $(a, b)$ si $k$ est clairement sous-entendu. Lorsque $a, b \in \mathbb{Q}^\times$ et $v \in V$, on écrit aussi $(a, b)_v$ pour préciser le corps $k = \mathbb{Q}_v$.

*3.1.2 - Remarques.* (i) En fait, ce symbole de Hilbert est défini sur les *corps $v$-adiques* $k = \mathbb{Q}_v$. Mais on l'a ici défini aussi pour $k = \mathbb{Q}$ puisque les discussions suivantes de ce numéro seront valables aussi pour $k = \mathbb{Q}$ que pour $k = \mathbb{Q}_v$.

(ii) Comme un facteur carré de $a$ (*resp.* $b$) peut être absorbé dans $x^2$ (*resp.* $y^2$), $(a,b)_k$ ne dépend pas de classes de $a, b$ dans $k^\times/k^{\times 2}$, donc définit une fonction binaire sur l'espace $\mathbf{F}_2$-vectoriel $k^\times/k^{\times 2}$ à valeur $\pm 1$. On a donc pour $a, c \in k^\times$

$$(a, c^2) = 1 \tag{3.1.2.1}$$

(iii) On voit que la définition est symétrique par rapport à $a$ et $b$, donc on a pour $a, b \in k^\times$

$$(a, b) = (b, a) \tag{3.1.2.2}$$

**3.1.3 (Groupe de normes).** Soit $K/k$ une extension finie de corps. Rappelons que l'on a une application $\mathrm{N}_{K/k} : K \to k$ appelée la *norme*, et qu'elle est *multiplicative* : $\mathrm{N}_{K/k}(xx') = \mathrm{N}_{K/k}(x)\mathrm{N}_{K/k}(x')$ pour tous $x, x' \in K$. On a $\mathrm{N}_{K/k}(a) = 0$ si et seulement si $a = 0$.

On notera $\mathrm{N}_{K/k}$ aussi pour l'ensemble $\mathrm{N}_{K/k}(K^\times)$ sans risque de confusion. C'est un sous-groupe (multiplicatif) de $k^\times$. On l'appelle le *groupe de normes de l'extension $K/k$*.

Soit $a \in k^\times$, on notera aussi $\mathrm{N}_{k,\sqrt{a}}$ pour le groupe $\mathrm{N}_{k(\sqrt{a})/k}$, qui ne dépend que de la classe de $a$ dans $k^\times/k^{\times 2}$. Si $a \in k^{\times 2}$, l'extension $k(\sqrt{a}) = k$ est triviale et on a $\mathrm{N}_{k,\sqrt{a}} = k^\times$ ; si $a \notin k^{\times 2}$, $k(\sqrt{a})/k$ est une extension quadratique et on a

$$\mathrm{N}_{k,\sqrt{a}} = \{x^2 - ay^2 : x, y \in k \text{ non tous zéros}\} \supseteq k^{\times 2} \tag{3.1.3.1}$$

Le symbole de Hilbert a une caractérisation par les normes des extensions quadratiques sur $k$, comme révèle la proposition suivante.

**3.1.4 - Proposition.** *Soit $a, b \in k^\times$. Alors $(a, b) = 1$ si et seulement si et seulement si $b \in \mathrm{N}_{k,\sqrt{a}}$.*

*Démonstration.* Si $a \in k^{\times 2}$, $(a, b) = 1$ (3.1.2.1) et $b \in \mathrm{N}_{k,\sqrt{a}}$ (3.1.3), l'équivalence est triviale. Si $a \in k^\times \backslash k^{\times 2}$, $(x, y, z) \in k^3$ est une solution non zéro de $z^2 - ax^2 - by^2 = 0$ si et seulement si $y \neq 0$ et $b = (zy^{-1})^2 - (xy^{-1})^2 = \mathrm{N}_{k(\sqrt{a})/k}(zy^{-1} + xy^{-1}\sqrt{a})$, d'où l'équivalence. □

**3.1.5 - Corollaire.** *Le symbole de Hilbert satisfait*

$$(a, b) = 1 \Rightarrow (a, c) = (a, bc) \tag{3.1.5.1}$$

$$(a, bc) = 1 \Rightarrow (a, b) = (a, c) \tag{3.1.5.2}$$

*En particulier, on a*

$$(a, b) = (a, -ab), \quad (a, ab) = (a, -b) \tag{3.1.5.3}$$

*Démonstration.* Selon (3.1.4), ces implications se traduisent comme

$$b \in \mathrm{N}_{k,\sqrt{a}} \Rightarrow \left(c \in \mathrm{N}_{k,\sqrt{a}} \Leftrightarrow bc \in \mathrm{N}_{k,\sqrt{a}}\right)$$

$$bc \in \mathrm{N}_{k,\sqrt{a}} \Rightarrow \left(b \in \mathrm{N}_{k,\sqrt{a}} \Leftrightarrow c \in \mathrm{N}_{k,\sqrt{a}}\right)$$

qui sont vrais puisque $\mathrm{N}_{k\sqrt{a}/k}$ est un groupe multiplicatif (3.1.3). En particulier, comme $-a = 0^2 - a \cdot 1^2 \in \mathrm{N}_{k,\sqrt{a}}$, on a donc $(a, b) = (a, (-a)b) = (a, -ab)$. En remplaçant $b$ par $-b$, on obtient l'autre identité de (3.1.5.3). □

## 3.2 *Démonstration du Théorème, cas* $n = 3$

*Démonstration du théorème de Hasse-Minkowski (cas $n = 3$).* Soit $f$ une forme quadratique sur $\mathbb{Q}$ non dégénérée de rang $n = 3$. On suppose que $f$ représente 0 dans $\mathbb{Q}_v$ pour tout $v \in V$ et on va démontrer que $f$ représente 0 aussi dans $\mathbb{Q}$. On a $f \sim Z^2 - aX^2 - bY^2$ à une constante non zéro près (1.5.3). Quitte à multiplier par des carrés de $\mathbb{Q}^\times$, on peut supposer que $a, b \in \mathbb{Z}\backslash\{0\}$ et qu'ils sont sans facteurs carrés ; alors $v_p(a), v_p(b) \in \{0, 1\}$ pour tout $p$ premier. Raisonnons par récurrence sur l'entier $m = |a| + |b|$ qui est toujours $\geq 2$.

Si $m = 2$, on a $a = \pm 1, b = \pm 1$. La résolubilité de $f = 0$ dans $\mathbb{R}$ exclut la possibilité $a = b = -1$, alors que dans les autres cas, $f$ représente bien 0.

Supposons alors $m > 2$. On peut d'abord supposer que $|a| \leq |b|$, cela entraîne $|b| \geq 2$. Donc $b$ possède au moins un facteur premier et on a

$$b = \pm \prod_{\substack{p \text{ premier} \\ p|a}} p$$

$a$ est un carré modulo $b$. En effet, pour tout $p$ divisant $b$, on a $v_p(b) = 1$ ; d'autre part, on a soit $a \equiv 0 \pmod{p}$, soit $v_p(a) = 0$ ; dans ce dernier cas, l'hypothèse que $f$ représente 0 dans $\mathbb{Q}_p$ entraîne que $a$ est un carré modulo $p$ (2.5.5). Enfin, on déduit que $a$ est un carré modulo $b$ selon le lemme chinois.

Cela étant, on peut trouver des entiers $t, b$ tels que $|t| \leq |b|$ et que $t^2 = a + bb'$. Alors, pour $k = \mathbb{Q}$ et $\mathbb{Q}_v$, on a $bb' = t^2 - a \cdot 1^2 \in \mathrm{N}_{k,\sqrt{a}}$ (3.1.3.1), alors $(a, bb')_k = 1$ (3.1.4), et puis $(a, b)_k = (a, b')_k$ (3.1.5.2). En posant $f' := Z^2 - aX^2 - b'Y^2$, on a donc

$$f \text{ représente 0 dans } \mathbb{Q} \, (\textit{resp.}\ \mathbb{Q}_v) \iff f' \text{ représente 0 dans } \mathbb{Q} \, (\textit{resp.}\ \mathbb{Q}_v)$$

Par l'hypothèse, $f$ représente 0 dans tous les $\mathbb{Q}_v$ ; l'équivalence par rapport à $\mathbb{Q}_v$ implique alors que $f'$ représente aussi 0 dans tous les $\mathbb{Q}_v$.

Remarquons en fin que $|b'| = \frac{|t^2 - a|}{|b|} < |b|$ en tenant compte que $|t| \leq |b|/2, |a| \leq |b|$ et $|b| \geq 2$. Par conséquent, $f'$ représente 0 dans $\mathbb{Q}$ en vertu de l'hypothèse de récurrence, l'équivalence ci-dessus par rapport à $\mathbb{Q}$ montre alors que $f$ représente aussi 0 dans $\mathbb{Q}$. □

## 3.3 Bilinéarité et non dégénérescence du symbol de Hilbert

**3.3.1 - Théorème** (Hilbert). *Le symbole de Hilbert $(\cdot, \cdot)_k$ est une forme bilinéaire non dégénérée sur le $\mathbf{F}_2$-espace vectoriel $k^\times/k^{\times 2}$, où $k = \mathbb{Q}_v$ pour $v \in V$.*

La proposition 3.1.4 nous permettra de déterminer le symbole de Hilbert en d'abord calculant les groupes de normes. Supposons maintenant $k = \mathbb{Q}_v$. L'ensemble des carrés non zéros $k^{\times 2}$ est un sous-groupe de $k^\times$ d'indice *fini* (2.4.4). On sait aussi (3.1.3) que $\mathrm{N}_{k,\sqrt{a}}$ est un sous-groupe de $k^\times$ contenant $k^{\times 2}$. Alors pour étudier le symbole de Hilbert sur $k = \mathbb{Q}_v$, on va d'abord calculer *cas par cas* les groupes de normes $\mathrm{N}_{k,\sqrt{a}}$ pour chaque $a$ représentant de classes dans $k^\times/k^{\times 2}$.

**3.3.2 - Proposition**. *On a des groupes de normes suivants :*

— *Cas* $k = \mathbb{Q}_\infty = \mathbb{R}$ *:* $\mathrm{N}_{\mathbb{R},\sqrt{-1}} = \mathbb{R}^{\times 2} = \mathbb{R}_+$ *;*

— *Cas* $k = \mathbb{Q}_2$ *:*

$$\mathrm{N}_{\mathbb{Q}_2,\sqrt{2}} = \mathbb{Q}_2^{\times 2}\{1,2,-1,-2\},\ \mathrm{N}_{\mathbb{Q}_2,\sqrt{-2}} = \mathbb{Q}_2^{\times 2}\{1,2,-5,-10\},\ \mathrm{N}_{\mathbb{Q}_2,\sqrt{-1}} = \mathbb{Q}_2^{\times 2}\{1,2,5,10\},$$
$$\mathrm{N}_{\mathbb{Q}_2,\sqrt{5}} = \mathbb{Q}_2^{\times 2}\{1,-1,5,-5\},\ \mathrm{N}_{\mathbb{Q}_2,\sqrt{-5}} = \mathbb{Q}_2^{\times 2}\{1,-2,5,-10\},$$
$$\mathrm{N}_{\mathbb{Q}_2,\sqrt{10}} = \mathbb{Q}_2^{\times 2}\{1,-1,10,-10\},\ \mathrm{N}_{\mathbb{Q}_2,\sqrt{-10}} = \mathbb{Q}_2^{\times 2}\{1,-2,-5,10\}\,;$$

— *Cas* $k = \mathbb{Q}_p$ *avec* $p \neq 2$ *premier,* $u \in \mathbb{Z}_p^\times \backslash \mathbb{Q}_p^{\times 2}$ *:*

$$\mathrm{N}_{\mathbb{Q}_p,\sqrt{p}} = \mathbb{Q}_p^{\times 2}\{1,-p\},\ \mathrm{N}_{\mathbb{Q}_p,\sqrt{u}} = \mathbb{Q}_p^{\times 2}\{1,u\},\ \mathrm{N}_{\mathbb{Q}_p,\sqrt{up}} = \mathbb{Q}_2^{\times 2}\{1,-up\}.$$

*Idée de la démonstration.* Pour donner un exemple, on calcule $\mathrm{N}_{\mathbb{Q}_2,\sqrt{-2}}$ :

(i) (Élément évident) Un élément de $\mathrm{N}_{\mathbb{Q}_2,\sqrt{-2}}$ est de la forme $x^2 - (-2)y^2$ où $x, y \in \mathbb{Q}_2$ ne s'annulent pas tous. On voit alors que $2 \in \mathrm{N}_{\mathbb{Q}_2,\sqrt{-2}}$.

(ii) (Éléments moins évidents) $-5 \in \mathrm{N}_{\mathbb{Q}_2,\sqrt{-2}}$ selon (2.5.7) ; comme $\mathrm{N}_{\mathbb{Q}_2,\sqrt{-2}}$ est un groupe, on a aussi $-10 = 2 \times (-5) \in \mathrm{N}_{\mathbb{Q}_2,\sqrt{-2}}$.

(iii) (Élément pas contenu dedans) $5 \notin \mathrm{N}_{\mathbb{Q}_2,\sqrt{-2}}$ selon (2.5.7).

On a donc $\{\overline{1}, \overline{2}, \overline{-5}, \overline{-10}\} \subset \mathrm{N}_{\mathbb{Q}_2,\sqrt{-2}}/\mathbb{Q}_2^{\times 2} \subsetneq \mathbb{Q}_2/\mathbb{Q}_2^{\times 2}$. Notons enfin que $\mathbb{Q}_2/\mathbb{Q}_2^{\times 2}$ est de cardinal 8 (2.4.4), donc son sous-groupe (3.1.3) $\mathrm{N}_{\mathbb{Q}_2,\sqrt{-2}}/\mathbb{Q}_2^{\times 2}$ est de cardinal 1,2,4 ou 8 d'après Lagrange. On en conclut que $\left|\mathrm{N}_{\mathbb{Q}_2,\sqrt{-2}}/\mathbb{Q}_2^{\times 2}\right| = 4$ et $\mathrm{N}_{\mathbb{Q}_2,\sqrt{-2}} = \mathbb{Q}_2^{\times 2}\{1,2,-5,-10\}$. □

**3.3.3 - Corollaire.** *Soit* $k = \mathbb{Q}_v$, $v \in V$. *On a une application bijective*

$$\begin{array}{ccc} (k^\times/k^{\times 2})\backslash\{1\} & \longrightarrow & \left\{ \begin{array}{c} \textit{sous-groupes de } k^\times \\ \textit{d'indice 2 et contenant } k^{\times 2} \end{array} \right\} \\ a & \longmapsto & \mathrm{N}_{k,\sqrt{a}} \end{array}$$

*Démonstration.* Cette application est bien définie (3.1.3). Elle est injective puisque les groupes de normes des classes d'équivalence différentes de $k^\times/k^{\times 2}$ sont distinctes (3.3.2). Elle est surjective car on peut énumérer explicitement l'ensemble à droite à l'aide de (2.4.4, (ii)). □

**3.3.4 - Corollaire.** *Soit* $k = \mathbb{Q}_p$, *et soient* $a, c \in k^\times, b, e \in k^\times \backslash k^{\times 2}$. *Pour que* $a\mathrm{N}_{k,\sqrt{b}}$ *et* $c\mathrm{N}_{k,\sqrt{e}}$ *soient disjoints, il faut et il suffit que* $be \in k^{\times 2}$ *et* $(ac, b) = -1$. *De plus, dans ce cas, on a*

$$a\mathrm{N}_{k,\sqrt{b}} \cup c\mathrm{N}_{k,\sqrt{e}} = k^\times \tag{3.3.4.1}$$

*Démonstration.* Notons d'abord que deux sous-groupes $H_1, H_2$ distincts d'un groupe $G$ d'indice 2 (donc $H_1, H_2$ sont des sous-groupes normaux) ne peuvent avoir de relation d'inclusion entre eux, sinon $[G : H_1] = [G : H_2]$ impliquera $H_1 = H_2$ ; alors $H_1$ intersecte $G\backslash H_2 = hH_2$ avec $h \notin H_2$ ; donc $H_1$ intersecte toutes les classes de $G/H_2$.

Par conséquent, comme $N_{k,\sqrt{b}}, N_{k,\sqrt{e}}$ sont d'indice 2 dans $k^\times$, pour que $a\mathrm{N}_{k,\sqrt{b}} \cap c\mathrm{N}_{k,\sqrt{e}} = \emptyset$, il faut et il suffit que $\mathrm{N}_{k,\sqrt{b}} = \mathrm{N}_{k,\sqrt{e}}$ et $a\mathrm{N}_{k,\sqrt{b}} \neq c\mathrm{N}_{k,\sqrt{b}}$, ou encore $b/e \in k^{\times 2}$ (3.3.3) et $a/c \notin \mathrm{N}_{k,\sqrt{b}}$, ou ce qui revient au même enfin que $be \in k^{\times 2}$ et $(ac, b) = (a/c, b) = -1$.

Si c'est le cas, comme $\mathrm{N}_{k,\sqrt{b}}$ est d'indice 2 dans $k^\times$, les conditions $\mathrm{N}_{k,\sqrt{b}} = \mathrm{N}_{k,\sqrt{e}}$ et $a\mathrm{N}_{k,\sqrt{b}} \neq c\mathrm{N}_{k,\sqrt{b}}$ implique que :

$a\mathrm{N}_{k,\sqrt{b}} \cup c\mathrm{N}_{k,\sqrt{e}}$ = la réunion (ensembliste) de toutes les classes de $k^\times/\mathrm{N}_{k,\sqrt{b}} = k^\times$ □

*3.3.5 - Remarque.* Si $(ac, b) = -1$, on a $b \notin k^{\times 2}$. Si de plus $be \in k^{\times 2}$, on a $e = b \cdot be \notin k^{\times 2}$. On obtient une version un peu différente du corollaire précédent :

*Soit $k = \mathbb{Q}_p$, et soient $a, b, c, e \in k^\times$. Pour que $b, e \in k^\times \backslash k^{\times 2}$ et $a\mathrm{N}_{k,\sqrt{b}}$ et $c\mathrm{N}_{k,\sqrt{e}}$ soient disjoints, il faut et il suffit que $be \in k^{\times 2}$ et $(ac, b) = -1$.*

*3.3.6 - Exemples.* Calculons quelques valeurs de $(\cdot,\cdot)_p$ où $p \neq 2$ :

(i) $(u,u)_p = 1$ et $(p,u)_p = -1$; (ii) $(p,p)_p = \left(\frac{-1}{p}\right)$; (iii) $(p,up)_p = -\left(\frac{-1}{p}\right)$;

(iv) $(up,up)_p = \left(\frac{-1}{p}\right)$; (v) $(p,l)_p = \left(\frac{l}{p}\right)$ où $l \neq p$ est un premier; (vi) $(2,p)_2 = (-1)^{\frac{p^2-1}{8}}$;

(vii) $(a,b)_2 = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}$ où $a, b$ sont des entiers impairs.

En effet :

(i) On observe que $u \in \mathbb{N}_{\mathbb{Q}_p,\sqrt{u}}$ et $p \notin \mathbb{N}_{\mathbb{Q}_p,\sqrt{u}}$ (3.3.2).

(ii) On a (3.1.5.3) $(p,p)_p = (p,-1)_p$ ; et ce dernier est égal à $\left(\frac{-1}{p}\right)$ selon l'exemple 2.5.5.

(iii) Comme $u \notin \mathrm{N}_{\mathbb{Q}_p,\sqrt{p}}$ et que $\mathrm{N}_{\mathbb{Q}_p,\sqrt{p}}$ est un sous-groupe de $\mathbb{Q}_p^\times$ d'indice 2 (3.3.2), on a $\mathbb{Q}_p^\times = \mathrm{N}_{\mathbb{Q}_p,\sqrt{p}} \amalg u\mathrm{N}_{\mathbb{Q}_p,\sqrt{p}}$, donc $(p,up) = -(p,p)$.

(iv) De plus, la multiplication par $u$ échange $\mathrm{N}_{\mathbb{Q}_p,\sqrt{up}}$ et $u\mathrm{N}_{\mathbb{Q}_p,\sqrt{up}}$, donc $(up,up) = -(p,up)$.

(v) On a $v_p(l) = 0$ (2.2.1). La formule résulte alors de (2.5.5) avec $a = l$.

(vi) On a $v_p(2) = 0$ (2.2.1), donc $p \notin (\pm 2)\mathbb{Q}_2^{\times 2}$, alors $p \in \mathbb{Q}_2^{\times 2} \amalg (-1)\mathbb{Q}_2^{\times 2} \amalg 5\mathbb{Q}_2^{\times 2} \amalg (-5)\mathbb{Q}_2^{\times 2}$, et plus particulièrement $p \in \mathbb{Z}_2^{\times 2} \amalg (-1)\mathbb{Z}_2^{\times 2} \amalg 5\mathbb{Z}_2^{\times 2} \amalg (-5)\mathbb{Z}_2^{\times 2}$. Alors $(2,p)_2 = 1$ équivaut à $p \in (\pm 1)\mathbb{Z}_2^{\times 2}$ (3.3.2), puis à $\pm p \equiv 1 \pmod 8$ (2.4.4), ou encore à $\frac{p^2-1}{8} \equiv 0 \pmod 2$.

(vii) Si $\frac{a-1}{2} \equiv 0 \pmod 2$, on a soit $a \equiv 1 \pmod 8$ et puis $a \in 1 + 8\mathbb{Z}_2 \subset \mathbb{Q}_2^{\times 2}$, soit $a \equiv 5 \pmod 8$ et puis $a \in 5(1+8\mathbb{Z}_2) \subset 5\mathbb{Q}_2^{\times 2}$ (2.4.4, (i)). De façon similaire, si $\frac{a-1}{2} \equiv 1 \pmod 2$, on a $a \in (-1)5\mathbb{Q}_2^{\times 2} \amalg (-1)\mathbb{Q}_2^{\times 2}$. De même pour $b$. D'autre part, on a $(-1,5) = (\pm 5, 5)_2 = 1$ et $(-1,-1)_2 = (-1,-5)_2 = (-5,-5)_2 = -1$ (3.3.2). La formule en résulte.

*3.3.7 - Remarque (Idée de la preuve du théorème 3.3.1).* $k^\times/k^{\times 2}$ étant un ensemble fini (2.4.4) pour $k = \mathbb{Q}_v$, on pourra calculer toutes les valeurs du symbole de Hilbert grâce à (3.1.4) et au calcul (3.3.2) et (3.3.6). On pourra ensuite vérifier explicitement la bilinéarité et la non dégénérescence. On obtiendra dans ce processus les matrices de la forme $\mathbf{F}_2$-bilinéaire :

— $v = \infty$ avec $\{\overline{-1}\}$ comme $\mathbf{F}_2$-base de $\mathbb{R}^\times/\mathbb{R}^{\times 2}$ :

$$(-1)$$

— $v = 2$ avec $\{\overline{2}, \overline{-1}, \overline{5}\}$ comme $\mathbf{F}_2$-base de $\mathbb{Q}_2/\mathbb{Q}_2^{\times 2}$ :

$$\begin{pmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 1 \end{pmatrix}$$

— $v = p \neq 2$ avec $\{\overline{u}, \overline{p}\}$ comme $\mathbf{F}_2$-base de $\mathbb{Q}_p/\mathbb{Q}_p^{\times 2}$, où $u \in \mathbb{Z}_p^\times \backslash \mathbb{Q}_p^{\times 2}$ :

$$\begin{pmatrix} 1 & -1 \\ -1 & \left(\frac{-1}{p}\right) \end{pmatrix}$$

## 3.4 Invariant de Hasse

Introduisons l'invariant de Hasse pour les formes quadratiques sur $k = \mathbb{Q}_v$.

**3.4.1 - Proposition** (Invariant de Hasse). *Soit $(V, Q)$ une forme quadratique* non dégénérée *sur $k = \mathbb{Q}_v$. Pour toute base* orthogonale $\mathscr{C} = (e_i)_{1\leq i\leq n}$, *posons $a_i = Q(e_i)$ et ensuite*

$$\varepsilon_{\mathscr{C}} = \prod_{1\leq i<j\leq n} (a_i, a_j) \tag{3.4.1.1}$$

*où par convention, on pose $\varepsilon_{\mathscr{C}} = 1$ si $n = 1$. Alors $\varepsilon_{\mathscr{C}}$ ne dépend pas du choix de $\mathscr{C}$, et est noté $\varepsilon(Q)$. Par conséquent, $\varepsilon(Q)$ est un invariant associé à $(V, Q)$, et est appelé l'*invariant de Hasse *de $Q$.*

On ne recopiera pas sa preuve, pour laquelle on pourra consulter [Ser77, Chap. IV, n° 2.1, Thm. 5]. Soit $f$ une forme quadratique usuelle non dégénérée sur $\mathbb{Q}_v$, on définit alors son invariant de Hasse comme $\varepsilon(f) = \varepsilon(Q_f)$.

**3.4.2 - Proposition** (Un critère de représentabilité). *Soit $f$ une forme quadratique non dégénérée de rang 2 sur $\mathbb{Q}_v$. Soit $x \in \mathbb{Q}_v^\times$. Alors, $f$ représente $x$ si et seulement si $(x, -d(f)) = \varepsilon(f)$. Autrement dit (1.5.5), $f \dot{-} xZ^2$ représente 0 si et seulement si $(x, -d(f)) = \varepsilon(f)$.*

*Démonstration.* On a (1.5.3) $f \sim aX^2 + bY^2, a, b \in \mathbb{Q}_v$. $f$ représente $x \in \mathbb{Q}_v^\times$ si et seulement si $xZ^2 - aX^2 - bY^2 = x\left(Z^2 - ax^{-1}X^2 - bx^{-1}Y^2\right)$ représente 0, si et seulement si $(ax^{-1}, bx^{-1}) = 1$. En utilisant la $\mathbf{F}_2$-bilinéarité et la symétricité, on obtient

$$(ax^{-1}, bx^{-1}) = (a, b)(a, x^{-1})(x^{-1}, b)(x^{-1}, x^{-1}) = (a, b)(x^{-1}, abx^{-1}) = (a, b)(x, abx)$$

Comme le symbole de Hilbert prend la valeur dans $\{\pm 1\}$, et en utilisant (3.1.5.3), on obtient

$$(a, b)(ax^{-1}, bx^{-1}) = (x, abx) = (x, -ab)$$

D'autre part, on a $d(f) = ab$ et $\varepsilon(f) = (a, b)$ par définition ; cela achèvera la preuve. □

**3.4.3 - Corollaire.** *Soit $f$ une forme quadratique non dégénérée de rang 3. $f$ est anisotrope si et seulement si $\varepsilon(f) = -(-1, -d(f))$.*

*Démonstration.* On a $f \sim aX^2 + bY^2 - xZ^2$ pour $a, b, x \in k^\times$. $f$ est anisotrope (i.e. $f$ ne représente pas 0) si seuelement si $(a, b) = -(x, -ab)$ (3.4.2). D'autre part, on a

$$\begin{aligned}
\varepsilon(f) &= (-x, a)(-x, b)(a, b) = (-x, ab)(a, b) && \text{(définition, bilinéarité)}\\
&= (-x, xab)(a, b) = (-1, xab)(x, xab)(a, b) && \text{((3.1.5.3), bilinéarité)}\\
&= (-1, -d(f))(x, -ab)(a, b) && (d(f) = -xab \text{ par définition})
\end{aligned}$$

Donc $f$ est anisotrope si et seulement si $\varepsilon(f) = -(-1, -d(f))$. □

## 3.5 Formule de produit

**3.5.1 - Théorème** (Formule de produit). *Si $a, b \in \mathbb{Q}^\times$, on a $(a, b)_v = 1$ pour presque tout $v \in V$ (i.e. sauf pour un nombre fini de $v$), et*

$$\prod_{v\in V} (a, b)_v = 1 \tag{3.5.1.1}$$

*Idée de la démonstration.* Tout élément de $\mathbb{Q}^\times$ se factorisant en un nombre fini de facteurs premiers et une signe $\pm$, il suffit de vérifier ce théorème pour $a, b$ égaux à $-1$ ou à un nombre premier. Pour cela, il ne nous reste que du calcul parce que l'on connaît déjà la structure multiplicative de $\mathbb{Q}_v^\times$ (2.4.4) et le symbole de Hilbert là-dessus (3.3.1) (3.3.6).

Explicitons un peu. Dans le cas où $a, b$ sont des nombres *premiers différents*, on peut supposer $b$ impair par la symétricité ; on a $(a,b)_v = 1$ pour tout $v \neq 2, a, b$ (3.3.6, (i)), et en vertu de (3.3.6, (v),(vi),(vii)), la formule de produit (3.5.1.1) équivaut à

$$(a,b)_2(a,b)_b(a,b)_a = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = 1 \qquad \text{si } a \text{ et } b \text{ sont impairs}$$

$$(a,b)_2(a,b)_b = (-1)^{\frac{b^2-1}{8}}\left(\frac{2}{b}\right) = 1 \qquad \text{si } a = 2 \text{ et } b \text{ est impair}$$

qui sont exactement la loi de réciprocité quadratique ! Si $a = -1$ et $b$ est un premier impair, (3.5.1.1) devient $(a,b)_2(a,b)_b = (-1)^{\frac{b-1}{2}}\left(\frac{-1}{b}\right) = 1$. C'est aussi le cas où $a = b$ est un premier impair car $(a,a)_v = (-1,a)_v$ pour tout $v \in V$ (3.1.5.3) . Enfin, en vertu de (3.3.6, (i)) et (3.3.7), $(2,2)_v = (2,-1)_v = 1$ pour tout $v \in V$, $(-1,-1)_v = -1$ si $v = \infty, 2$, et $(-1,-1)_v = 1$ sinon. □

Compte tenu de l'équation de définition de l'invariant de Hasse (3.4.1.1), on obtient

**3.5.2 - Corollaire.** *Soit $f$ une forme quadratique sur $\mathbb{Q}$. Pour tout $v \in V$, $f$ devient une forme quadratique sur $\mathbb{Q}_v$ (1.5.8), dont l'invariant de Hasse correspondant sera noté $\varepsilon_v(f)$. On a $\varepsilon_v(f) = 1$ pour presque tout $v \in V$, et*

$$\prod_{v \in V} \varepsilon_v(f) = 1$$

Il est naturel de poser la question inverse suivante : dans quelle mesure est-ce que l'on peut trouver une solution dans $\mathbb{Q}^\times$ pour un système d'équations dans les $\mathbb{Q}_v^\times$ ? Il se trouve que les conditions nécessaires imposées par (3.5.2) (la trivialité du symbole presque partout, la formule de produit, et la résolubilité dans chaque $\mathbb{Q}_v^\times$) suffisent déjà, comme précisé ci-après.

**3.5.3 - Théorème** (Existence, résolubilité). *Soit $(a_i)_{i \in I}$ une famille finie d'éléments de $\mathbb{Q}^\times$, et soit $(\varepsilon_{i,v})_{i \in I, v \in V}$ une famille de nombres $\pm 1$. Pour qu'il existe $x \in \mathbb{Q}^\times$ tel que*

$$(x, a_i)_v = \varepsilon_{i,v} \quad \forall i \in \mathrm{I}, v \in V$$

*il faut et il suffit que les trois conditions suivantes soient satisfaisantes :*

*(i) Pour tout $i \in I$, on a $\varepsilon_{i,v} = 1$ pour presque tout $v \in V$ ;*

*(ii) Pour tout $i \in I$, on a la formule de produit $\prod_{v \in V} \varepsilon_{i,v} = 1$ ;*

*(iii) Pour tout $v \in V$, il existe $x_v \in \mathbb{Q}_v^\times$ tel que*

$$(x_v, a_i)_v = \varepsilon_{i,v} \quad \forall i \in \mathrm{I}$$

La nécessité résulte de (3.5.2). Pour la suffisance, il y a une très jolie preuve basée sur le théorème de la progression arithmétique de Dirichlet, pour laquelle nous renvoyons le lecteur à [Ser77, Chap. III, n° 2.2, Thm. 4].

## 3.6 *Démonstration du Théorème, cas* $n = 4$

*Démonstration du théorème de Hasse-Minkowski (cas $n = 4$).* Soit $f$ une forme non dégénérée de rang $n = 4$ sur $\mathbb{Q}$ représentant 0 dans $\mathbb{Q}_v$ pour tout $v \in V$. $f$ étant diagonalisable (1.5.3), on peut écrire $f = g \dot{-} h$ où $g, h$ sont des formes non dégénérées de rang 2. Par l'hypothèse et (1.5.6), pour tout $v \in V$, il existe $x_v \in \mathbb{Q}_v^\times$ représenté à la fois par $g$ et $h$ dans $\mathbb{Q}_v$, alors d'après (3.4.2), on a pour tout $v \in V$

$$(x_v, -d(g))_v = \varepsilon_v(g)$$
$$(x_v, -d(h))_v = \varepsilon_v(h)$$

On sait (3.5.2) que $\varepsilon_v(g) = \varepsilon_v(h) = 1$ pour presque tous les $v \in V$ et que $(\varepsilon_v(g))_{v\in V}$ et $(\varepsilon_v(h))_{v\in V}$ satisfont à la formule de produit. Donc selon (3.5.3), il existe $x \in \mathbb{Q}^\times$ tel que pour tout $v \in V$, on a

$$(x, -d(g))_v = \varepsilon_v(g)$$
$$(x, -d(h))_v = \varepsilon_v(h)$$

Alors, $g \dot{-} xZ^2$ et $h \dot{-} xZ^2$ représentent 0 dans tout $\mathbb{Q}_v$ (3.4.2), donc aussi dans $\mathbb{Q}$ selon le cas $n = 3$ du théorème Hasse-Minkowski. Ainsi (1.5.5), $g, h$ toutes deux représentent $x$ dans $\mathbb{Q}$, donc (1.5.6) $f = g \dot{-} h$ représente 0 dans $\mathbb{Q}$. □

# 4 Formes quadratiques sur $\mathbb{Q}_v$ : classification

La proposition 3.4.2 a donné un premier exemple du critère de représentabilité d'un élément de $\mathbb{Q}_v$ par une forme quadratique de rang 2 sur $\mathbb{Q}_v$. Plus généralement, on pourra donner une classification d'équivalence de formes quadratiques (non dégénérées) sur $\mathbb{Q}_v$, selon la signature, ou selon le rang, le discriminant et l'invariant de Hasse.

On sait aussi qu'une forme quadratique est déterminée à équivalence près par son indice d'isotropie et son noyau anisotrope (1.5.7). Donc on va particulièrement s'intéresser aux formes *anisotropes*.

## 4.1 Formes quadratiques sur $\mathbb{R}(= \mathbb{Q}_\infty)$

**4.1.1 - Théorème** (Loi d'inertie de Sylvester, signature). *Soit $(V, Q)$ une forme quadratique non dégénérée sur $\mathbb{R}$, alors il existe une base orthogonale $\mathcal{E} = (e_i)_{1\le i\le n}$ et $r, s \in \mathbb{N}$ telle que $r + s = n$, $Q(e_1) = \ldots = Q(e_r) = 1$, $Q(e_{r+1}) = \ldots = Q(e_{r+s}) = -1$. De plus, la paire $(r, s)$ est uniquement déterminée, et est appelée la* signature *de $(V, Q)$.*

*Démonstration.* Selon le théorème de base orthogonale (1.2.3), quitte à normaliser les coefficients non zéros en $\pm 1$, il existe une base orthogonale $\mathcal{E} = (e_i)_{1\le i\le n}$ et $r, s \in \mathbb{N}$ tels que $Q(e_1) = \ldots = Q(e_r) = 1$, $Q(e_{r+1}) = \ldots = Q(e_{r+s}) = -1$, $Q(e_i) = 0$ pour $r + s < i \le n$ ; et on a $r + s = n$ car $V$ est non dégénéré, d'où l'existence. Pour l'unicité, montrons la caractérisation suivante de $(r, s)$ (où $\subset$ désigne un sous-espace vectoriel) invariante sous isomorphismes :

$$r = \max\{\dim W_+ : W_+ \subset V,\ Q \text{ est positive définie sur } W_+\}$$
$$s = \max\{\dim W_- : W_- \subset V,\ Q \text{ est négative définie sur } W_-\}$$

En effet, soient $W_+, W_-$ des sous-espaces vectoriels maximisant ci-dessus à droite. On a

$$r \leq \dim W_+ \tag{4.1.1.1}$$
$$s \leq \dim W_- \tag{4.1.1.2}$$

puisque $Q$ est positive définie sur $\mathrm{Vect}(e_1, \ldots, e_r)$ et négative définie sur $\mathrm{Vect}(e_{r+1}, \ldots, e_{r+s})$. D'autre part, on a $W_+ \cap W_- = \{0\}$ par la positivité et la négativité définies ; par suite, $n = r + s \leq \dim(W_+ \oplus W_-) \leq \dim V = n$. Il en résulte que (4.1.1.1) et (4.1.1.2) sont en fait des égalités. L'unicité en découle aussitôt. □

**4.1.2 - Théorème** (Classification). *Deux formes quadratiques non dégénérées sur $\mathbb{R}$ sont équivalentes si et seulement si elles ont la même signature.*

*Démonstration.* D'une part, la signature est un invariant de telles formes quadratiques (1.1.4) (4.1.1) ; d'autre part, toutes les formes non dégénérées ayant signature $(r, s)$ sont par définition (4.1.1) équivalentes à la forme $X_1^2 + \ldots + X_r^2 - X_{r+1}^2 - \ldots - X_{r+s}^2$. □

**4.1.3 - Corollaire** (Formes anisotropes). *Une forme quadratique non dégénérée sur $\mathbb{R}$ de signature $(r, s)$ est anisotrope si et seulement si $rs = 0$, i.e. elle est négative définie ou positive définie.* □

## 4.2 Formes quadratiques sur $\mathbb{Q}_p$

Dans tout ce numéro, posons $k = \mathbb{Q}_p$, et soit $f$ une forme quadratique sur $k$ non dégénérée de rang $n \geq 1$, de discriminant $d = d(f)$ et d'invariant de Hasse $\varepsilon = \varepsilon(f)$.

**4.2.1 - Théorème** (Formes anisotropes). *Pour que $f$ soit anisotrope, il faut et il suffit que :*

- *$n = 1$ et $\varepsilon = 1$ ;*
- *$n = 2$ et $d \neq -1 \in k^\times/k^{\times 2}$ ;*
- *$n = 3$ et $\varepsilon = -(-1, -d)$ ;*
- *$n = 4$ et $d = 1 \in k^\times/k^{\times 2}$, $\varepsilon = -(-1, -1)$.*

*En particulier, toutes les formes de rang $\geq 5$ sont isotropes.*

*Démonstration du théorème 4.2.1.* ⋆ — Si $n = 1$, $f = aX^2$ ($a \in k^\times$) est toujours anisotrope ; on a $\varepsilon = 1$ et il n'y a aucune contrainte sur $d = a$.

⋆ — Si $n = 2$, $f \sim a(X^2 - bY^2)$, $d = -a^2 b$ ; $f$ est anisotrope si et seulement si $b \notin k^{\times 2}$, donc si et seulement si $d \neq -1$ dans $k^\times/k^{\times 2}$.

**4.2.1.1 - Corollaire.** *Si $n \geq 2$, $f$ représente au moins deux classes de $k^\times/k^{\times 2}$.*

*Démonstration de (4.2.1.1).* $f$ étant diagonalisable (1.5.3), il suffit de démontrer pour $n = 2$. Si $f \sim a(X^2 - bY^2)$ est anisotrope, elle représente les éléments de $a\mathrm{N}_{k,\sqrt{b}}$ (3.1.3), donc parmi les classes de $k^\times/k^\times$, $f$ représente $a\left(\mathrm{N}_{k,\sqrt{-d}}/k^{\times 2}\right)$, qui est de cardinal (2.4.4, (ii)) (3.3.3)

$$\left|\mathrm{N}_{k,\sqrt{-d}}/k^{\times 2}\right| = \left|k^\times/k^{\times 2}\right| \Big/ \left|k^\times/\mathrm{N}_{k,\sqrt{-d}}\right| = \begin{cases} 2 & \text{si } k = \mathbb{Q}_p,\ p \neq 2 \\ 4 & \text{si } k = \mathbb{Q}_2 \end{cases}$$

Donc $f$ représente au moins deux classes de $k^\times/k^{\times 2}$. Si au contraire $f$ est isotrope, alors $f$ représente $k$ (1.5.4), *a fortiori* représente toutes les classes de $k^\times/k^{\times 2}$ ($\geq 4$ (2.4.4, (ii))). □

Revenons à la démonstration du théorème.

★ — Le cas $n = 3$ a été fait dans (3.4.3).

★ — Si $n = 4$, $f \sim a(X^2 - bY^2) - c(Z^2 - eW^2) = aX^2 - abY^2 - cZ^2 + ceW^2$ $(a, b, c, e \in k^\times)$. Pour que $f$ soit anisotrope, il faut et il suffit que $a(X^2 - bY^2)$ et $c(Z^2 - eW^2)$ soient anisotropes et qu'elles ne représentent aucun élément commun de $k^\times$ (1.5.6), ce qui revient au même que

$$b, e \in k^\times \backslash k^{\times 2} \text{ et } a\mathrm{N}_{k,\sqrt{b}} \cap c\mathrm{N}_{k,\sqrt{e}} = \emptyset \tag{4.2.1.2}$$

ou encore (3.3.5)

$$be \in k^{\times 2} \text{ et } (ac, b) = -1 \tag{4.2.1.3}$$

D'autre part, en faisant du calcul, on obtient

$$d(f) = a(-ab)(-c)ce = be \in k^\times / k^{\times 2} \tag{4.2.1.4}$$

et

$$\begin{aligned}
\varepsilon(f) &= (a, -ab)(a(-ab), (-c)ce)(-c, ce) && \text{(définition)} \\
&= (a, b)(-b, -e)(ce, -c) && \text{(éliminer les carrés)} \\
&= (a, b)\left[(-1, -1)(b, -1)(-1, e)(b, e)\right](ce, (-ce)(-c)) && \text{(bilinéarité, (3.1.5.3))} \\
&= (a, b)(-1, -1)(-1, be)(b, e)(ce, e) && \text{(bilinéarité, éliminer le carré)} \\
&= (a, b)(-1, -1)(-1, be)(b, e)\left[(c, e)(e, e)\right]\left[(b, c)(b, c)\right] && \text{(bilinéarité, } (\cdot, \cdot) = \pm 1\text{)} \\
&= (a, b)(-1, -1)(-1, be)(ce, be)(b, c) && \text{(bilinéarité)} \\
&= (ac, b)(-1, -1)(-ce, be) && \text{(bilinéarité)}
\end{aligned}$$

d'où

$$\varepsilon = (ac, b)(-1, -1)(-ce, d) \tag{4.2.1.5}$$

Maintenant, il est facile de vérifier à l'aide de (4.2.1.4) et (4.2.1.5) que (4.2.1.3) est équivalente à $d = 1$, $\varepsilon = -(-1, -1)$, ce qui achève la preuve du cas $n = 4$.

★ — Si $n \geq 5$, $f \sim \sum_{i=1}^{n} a_i X_i^2$ représente les éléments qui sont déjà représentés par la forme non dégénérée $a_1 X_1^2 + \ldots + a_5 X_5^2$, donc il suffit de montrer que si $n = 5$, $f$ est isotrope. D'abord, il existe $a \in k^\times$ tel que $a \notin d(f)k^{\times 2}$ et que $f$ représente $a$ (4.2.1.1). Alors $f \sim g \dot{+} aZ^2$ (1.5.5) avec $g$ une forme non dégénérée de rang $n - 1 = 4$. Comme $d(g) = d(f)/a \neq 1$ dans $k^\times / k^{\times 2}$, $g$ est isotrope selon le cas de rang 4, donc *a fortiori* $f$ est isotrope. □

**4.2.2 - Corollaire** (Critère de représentabilité). *Soit $x \in k^\times$. $f$ représente $x$ si et seulement si*

- *$n = 1$ et $x = d$ ;*
- *$n = 2$ et $\varepsilon = (x, -d)$ ;*
- *$n = 3$ et, soit $x \neq -d$, soit $x = -d$ et $\varepsilon = (-1, -d)$.*
- *$n \geq 4$.*

*Démonstration.* Posons $g = f \dot{-} xZ^2$, qui est une forme non dégénérée de rang $n + 1$. On a

$$d(g) = -xd(f) \text{ et } \varepsilon(g) = (-x, d(f))\varepsilon(f) \tag{4.2.2.1}$$

Appliquons (4.2.1) à $g$ et utilisons (4.2.2.1), et le corollaire en découle. □

**4.2.3 - Corollaire.** *Deux formes quadratiques non dégénérées ayant le même rang, le même discriminant et le même invariant de Hasse représentent exactement les mêmes éléments de $k$.*

*Démonstration.* Deux telles formes représentent 0 ou non en même temps (4.2.1) ; elles représentent aussi les mêmes éléments $x \in k^\times$, tous les critères dans (4.2.2) concernant seulement le rang $n$, le discriminant $d$ et l'invariant de Hasse $\varepsilon$ (et $x$). □

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

*Démonstration.* La condition est nécessaire car ce sont des invariants par rapport à la relation d'équivalence. Pour la suffisance, raisonnons par récurrence sur le rang $n$.

Si $n = 1$, $f = aX^2$, $a = d(f) \in k^\times/k^{\times 2}$. Donc $f$ est determinée à èquivalence près par $d(f)$. Supposons $n \geq 2$, et soient $f, f'$ deux formes non dégénérées de mêmes invariants $n, d, \varepsilon$. Prenons un $x \in k^\times$ représenté par $f$, alors $g$ représente aussi $x$ (4.2.3). Alors

$$f \sim g \dotplus xZ^2 \text{ et } f' \sim g' \dotplus xZ^2$$

où $g$ et $g'$ sont non dégénérées de rang $n-1$. Il suffit alors de montrer que $g \sim g'$. Pour cela, on a (4.2.2.1)

$$d(g) = d(f)/x = d(f')/x = d(g')$$

et puis

$$\varepsilon(g) = \varepsilon(f)/(x, d(g)) = \varepsilon(f')/(x, d(g')) = \varepsilon(g)$$

Donc par l'hypothèse de récurrence appliquée à $g$ et $g'$, on obtient $g \sim g'$. □

*4.2.5 - Remarques.* (i) Ce théorème montre que (4.2.1) donne une « classification » au sens où pour chaque $(n, d, \varepsilon)$ satisfaisant les conditions de (4.2.1), il existe *au plus une* forme à èquivalence près ayant ces invariants. Nous allons voir que pour chaque tel $(n, d, \varepsilon)$, il *existe au moins une* forme ayant ces invariants, et nous allons les déterminer.

Lorsque $p \neq 2$, on a posé $u \in \mathbb{Z}_p^\times$ un élément non carré modulo $p$ ; si $p = 2$, posons maintenant $u = 5$, de sorte que l'on a $(u, p)_p = -1$ pour tout premier $p$ (3.3.7). Alors,

*Toutes les classes d'équivalence des formes anisotropes sur $\mathbb{Q}_p$ sont listées ci-dessous à droite et sont classifiées exclusivement par les données à gauche comme suivantes :*

$$\begin{array}{ll} n = 1,\ d \in k^\times/k^{\times 2} & f \sim dX^2 \\ n = 2,\ d \in \left(k^\times/k^{\times 2}\right)\backslash\{-1\},\ \overline{a} \in k^\times/\mathrm{N}_{k,\sqrt{-d}} & f \sim a(X^2 + dY^2) \\ n = 3,\ d \in k^\times/k^{\times 2} & f \sim -pd(X^2 - uY^2 + upZ^2) \\ n = 4 & f \sim X^2 - pY^2 - uZ^2 + upW^2 \end{array} \tag{4.2.5.1}$$

Remarquons que par rapport aux conditions de (4.2.1), on a supprimé, par exemple, la condition $\varepsilon = 1$ pour $n = 1$ et la condition $\varepsilon = -(-1, -d)$ pour $n = 3$, parce que $\varepsilon$ y est alors un paramètre redondant pour la classification. De même idée, même si $d$ est « sans contrainte » pour $n = 1$ dans (4.2.1), on l'a écrit pour spéficier l'ensemble de ses valeurs possibles pour que ce soit un paramètre de classification.

Vérifions la classification (4.2.5.1). Il suffit de vérifier que les formes à droite sont anisotropes d'invariants différents, et que ces invariants parcourent toutes les possibilités données par (4.2.1) :

— Si $n = 1$, pour tout $d \in k^\times/k^{\times 2}$, $dX^2$ est anisotrope. Par convention, $\varepsilon = 1$.

— Si $n = 2$ et $d \neq -1 \in k^\times/k^{\times 2}$, $a(X^2 + dY^2)$ est anisotrope (4.2.1). $k(\sqrt{-d})/k$ est une extension quadratique (3.1.3). On a $\varepsilon = (a, ad) = (a, -d) = 1$ si $a \in \mathrm{N}_{k,\sqrt{-d}}$, et on a $\varepsilon = -1$ sinon (3.1.4).

— Si $n = 3$, $-pd(X^2 - uY^2 + upZ^2) = -pd\big(X^2 - (uY^2 - upZ^2)\big)$ est anisotrope par la définition du symbole de Hilbert (3.1.1) car $(u, -up)_p = (u, p)_p = -1$ (3.3.7). D'ailleurs, son discriminant est $(-pd)^3(-u)(up) = d$.

— Si $n = 4$, $X^2 - pY^2 - uZ^2 + upW^2 = (X^2 - pY^2) - u(Z^2 - pW^2)$ est anisotrope d'après le critère (4.2.1.2) et le calcul des groupes de normes (3.3.2). D'ailleurs, il n'y a qu'une forme anisotrope de rang 4 (4.2.1).

(ii) Comme une conséquence de (4.2.5.1), si on note $r := \left|k^\times/k^{\times 2}\right|$ (donc $r = 4$ si $p \neq 2$, $r = 8$ si $p = 2$ (2.4.4)) et si on note $N_n^{an}$ le nombre de classes d'équivalence des formes *anisotropes* de rang $n$, on a

$$N_1^{an} = r, \quad N_2^{an} = 2(r-1), \quad N_3^{an} = r, \quad N_4^{an} = 1, \quad N_n^{an} = 1,\ n \geq 5 \tag{4.2.5.2}$$

Ensuite, en notant $N_n$ le nombre de classes d'équivalence des formes *non dégénérées* de rang $n$, on obtient $N_0 = 1$, et d'après la décomposition (1.5.7), $N_1 = N_1^{an} = r$ et

$$N_n = N_n^{an} + N_{n-2}^{an} + \ldots = N_n^{an} + N_{n-2},\ n \geq 2$$

d'où

$$N_0 = 1, \quad N_1 = r, \quad N_2 = 2r - 1, \quad N_n = 2r,\ n \geq 3 \tag{4.2.5.3}$$

Les représentants exacts des formes de rang $n$ donné pourront se déduire de la classification (4.2.5.1) et de la décomposition (1.5.7).

# Références


[Lub] Lubin. Kernel of $p$-adic logarithm. Mathematics Stack Exchange. https://math.stackexchange.com/q/333766 (version : 2013-03-18).

[Ser77] J.P. Serre. *Cours d'arithmétique*. Le Mathématicien. Presses Universitaires de France, 1977.