Département de mathématiques

Travail Encadré de Recherche

FORMES QUADRATIQUES SUR $\mathbb{Q}$

Maximilien WANG, Benjamin DA SILVA, Guilhem MUREAU

Sous la direction d'Olivier BRINON

2020-2021

Introduction

La classification des espaces quadratiques (V, q) sur un corps commutatif K consiste à décrire les classes d'isomorphismes (isométries bijectives) d'espaces quadratiques sur K (ou plus généralement des modules quadratiques sur un anneau commutatif). Une telle description est donnée par la liste complète des invariants de q pour la relation de similitude, à laquelle il faut ajouter la dimension de l'espace, qui est un invariant évident.
Nous connaissons les invariants des formes quadratiques sur quelques corps usuels : pour un corps commutatif algébriquement clos (par exemple $K = \mathbb{C}$), le rang est le seul invariant. Pour $K = \mathbb{R}$, la signature de l'espace quadratique vient s'ajouter au rang ; c'est le théorème d'inertie de Sylvester. Sur un corps fini (de caractéristique $\neq 2$), deux formes quadratiques sont isomorphes si et seulement si elles ont même rang et même discriminant. Dans l'étude de ces trois exemples, il apparaît que la classification est intimement liée à la structure du groupe des carrés du corps.

L'objet de ce mémoire est de classifier les formes quadratiques sur le corps des rationnels $\mathbb{Q}$. Puisque toute forme rationnelle est une forme réelle, nous pouvons déjà donner des invariants : le rang et la signature de la forme (vue comme forme quadratique sur $\mathbb{R}$). Toutefois le problème est plus complexe que sur $\mathbb{R}$ (tout comme le groupe des carrés de $\mathbb{Q}$ est plus complexe que celui de $\mathbb{R}$), nous aurons besoin de définir d'autres extensions de $\mathbb{Q}$ dans lesquelles plonger les formes quadratiques rationnelles : les corps p-adiques $\mathbb{Q}_p$. Il nous faudra ensuite faire la liste des invariants des formes sur les corps $\mathbb{Q}_p$. Enfin, le célèbre théorème de *Hasse-Minkowski* apportera la réponse à notre problème, en illustrant le *principe local-global.*

Nos remerciements s'adressent à notre tuteur Olivier Brinon, professeur des universités à l'Institut de Mathématiques de Bordeaux, pour ses conseils, ses relectures, sa bienveillance, et les petites astuces sur LaTeX. Merci à Alexandre Bailleul, AGPR à l'ENS de Paris-Saclay, pour les discussions sur le symbole de Hilbert. Nous remercions également Jean-Pierre Serre pour son fameux *Cours d'Arithmétique*.

Table des matières

1 Apéritif

1.1 Rappels sur les corps finis-compléments

Dans ce qui suit, les corps considérés seront supposés finis et commutatifs.

Définition 1.1.1. On appelle *corps premiers* les corps $\mathbb{Q}$ et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, avec p premier. On définit la *caractéristique d'un corps* K, notée $\mathrm{Car}(K)$, l'entier 0 ou p suivant que K est une extension de $\mathbb{Q}$ ou de $\mathbb{F}_p$.

Lemme 1.1.1. Si $\mathrm{Car}(K) = p$, l'application $\sigma : x \mapsto x^p$ est un isomorphisme (morphisme de Frobenius) de K.

Démonstration : On a évidemment $\sigma(xy) = \sigma(x)\sigma(y)$ (on suppose le corps commutatif). Soient $x, y \in K$, $\sigma(x+y) = \sum_{k=0}^{p} \binom{p}{k} x^k y^{n-k}$ et pour tout $1 < k < p$, $\binom{p}{k} = 0 \pmod p$. Donc : $\sigma(x+y) = \sigma(x) + \sigma(y)$. σ est donc un morphisme évidemment injectif (comme tout morphisme de corps). □

Théorème 1.1.1. *La caractéristique d'un corps fini K est un nombre premier $p \neq 0$. Si $f = [K : \mathbb{F}_p]$ alors K contient p^f éléments et est isomorphe à $\mathbb{F}_p$.*

Démonstration : Si K est un corps fini alors il ne saurait contenir $\mathbb{Q}$, sa caractéristique est donc un nombre premier $p \neq 0$. Si f est le degré de l'extension $K/\mathbb{F}_p$ alors il est clair que $|K| = p^f$. □

Lemme 1.1.2. Soit K un corps commutatif, soit G un sous-groupe fini du groupe multiplicatif $K^\times$. Alors G est un groupe cyclique.

Démonstration : Soit $n = |G|$. Pour tout entier $d \geq 1$, notons $G_d := \{x \in G \mid x^d = 1\}$ et $H_d \subset G_d$ le sous-ensemble des éléments d'ordre exactement d. On a alors $G = G_n$ est la réunion disjointe des H_d, $d \mid n$. Soit φ la fonction indicatrice d'Euler. Rappelons d'abord que $n = \sum_{d|n} \varphi(d)$.

Soit $d \mid n$ tel que $H_d \neq \emptyset$. Montrons que $|H_d| = \varphi(d)$. Pour tout diviseur e de d, on a $H_e \neq \emptyset$. De plus, $|H_e| \geq \varphi(e)$. En effet, si $a \in H_e$ (donc d'ordre e), alors les a^r avec $1 \leq r \leq e-1$ premiers à e sont deux à deux distincts et d'ordre e. Comme le polynôme $X^d - 1 \in K[X]$ a au plus d racines dans K, on a :

$$d \geq |G_d| = \sum_{e|d} |H_e| \geq \sum_{e|d} \varphi(e) = d$$

Donc $|H_e| = \varphi(e)$ pour tout $e \mid d$. En particulier, $|H_d| = \varphi(d)$. Il vient :

$$\sum_{d|n} \varphi(d) = n = |G| = \sum_{\substack{d|n \\ H_d \neq \emptyset}} \varphi(d)$$

Cela implique que $H_d \neq \emptyset$ pour tout $d \mid n$. Par conséquent, $H_n \neq \emptyset$, ce qui veut dire que G a un élément d'ordre n et est donc cyclique. $\square$

Théorème 1.1.2. *Le groupe multiplicatif $\mathbb{F}_q^\times$ du corps fini $\mathbb{F}_q$ est cyclique d'ordre $q-1$.*

Démonstration : On applique le lemme précédent à $\mathbb{F}_q$ et $\mathbb{F}_q^\times$ et on obtient que $\mathbb{F}_q^\times$ est cyclique d'ordre $\varphi(q) = q-1$. $\square$

Fixons un corps K de cardinal $q = p^r$ (donc de caractéristique p), $r \in \mathbb{N}_{>0}$.

Proposition 1.1.1. Soit K un corps tel qu'énoncé précédemment, alors :

(i) Si $K \subset K'$ est une extension finie, il existe $\xi \in K$ tel que $K' = K[\xi]$;

(ii) Si L est un sous-corps de K, alors $|L| = p^d$ avec $d \mid r$;

(iii) Soit $d \in \mathbb{N}^*$ divisant r, il existe un unique sous-corps L de K tel que $|L| = p^d$. On a $L = \{x \in K \mid x^{p^d} = x\}$ et L est isomorphe à $\mathbb{F}_{p^d}$.

Démonstration : (i) Comme K' est un corps fini, $K'^\times$ est cyclique. Si ξ est un générateur de ce groupe, il est clair que $K' = K[\xi]$.
(ii) Posons $|L| = n$, il existe $d \in \mathbb{N}^*$ tel que $n = p^d$. D'autre part, K étant un L-espace vectoriel de dimension finie, on a $q = n^s$ avec $s \in \mathbb{N}^*$ et on a fini.
(iii) Comme d divise r, $p^d - 1$ divise $p^r - 1 = q - 1$. Ecrivons $q - 1 = n(p^d - 1)$, et soit ξ un générateur du groupe cyclique $K^\times$. Alors ξ^n est d'ordre $p^d - 1$ et le sous-groupe G de $K^\times$ engendré par ξ^n est l'ensemble des $x \in K^\times$ qui vérifient $x^{p^d-1} = 1$. On a $|G| = p^d - 1$. Notons alors $K' = \{0\} \cup G$ est l'ensemble des éléments x de K tels que $x^{p^d} = x$ et $|K| = p^d$.
Posons $\tau : \left\{ \begin{array}{ccc} K & \to & K \\ x & \mapsto & x^{p^d} \end{array} \right.$. On a $\tau = (\sigma)^d$ (σ le morphisme de Frobenius). Ainsi, K' est un corps. Il existe donc un sous-corps de K de cardinal p^d. $\square$

Lemme 1.1.3. Soit $u \in \mathbb{N}$,

$$S(X^u) := \sum_{x \in K} x^u = \left\{ \begin{array}{ll} -1 & \text{si } u \geq 1 \quad \text{et divisible par} \quad q-1 \\ 0 & \text{sinon} \end{array} \right.$$

Démonstration : Si $u = 0$ alors tous les termes de la sommes valent 1 et on a alors : $S(X^u) = q \times 1 = 0$ puisque K est de caractéristique p et $q = p^r$.
Si $u \geq 1$ et divisible par $q - 1$, on a $0^u = 0$ et $x^u = 1$ si $x \neq 0$, d'où :

$$S(X^u) = (q-1) \times 1 = -1$$

Enfin, si $u \geq 1$ et non-divisible par $q - 1$, le fait que $K^\times$ soit cyclique d'ordre $q - 1$ montre qu'il existe $y \in K^\times$ tel que $y^u \neq 1$. On a :

$$S(X^u) = \sum_{x \in K^\times} x^u = \sum_{x \in K^\times} y^u x^u = y^u S(X^u)$$

D'où $(1-y^u)S(X^u)=0$, ce qui implique que $S(X^u)=0$. $\square$

Théorème 1.1.3. *(Chevalley-Warning) Soient A un ensemble fini et :*

$$f_\alpha \in K[X_1,...,X_n] \quad (\alpha \in A)$$

des polynômes à n variables tels que $\sum\limits_{\alpha\in A} \deg(f_\alpha) < n$, et soit V l'ensemble des zéros communs dans K^n. On a :

$$|V| = 0 \pmod p$$

Démonstration : Posons $P = \prod\limits_{\alpha}(1-f_\alpha^{q-1})$, et soit $x \in K^n$. Si $x \in V$ tous les $f_\alpha(x)$ sont nuls et donc $P(x)=1$; si $x \notin V$, l'un des $f_\alpha(x)$ est non nul, et $f_\alpha^{q-1}(x)=1$ d'où $P(x)=0$. Ainsi, P est la fonction caractéristique de V. Si, pour tout polynôme f, on pose $S(f) = \sum\limits_{x\in K^n} f(x)$, on a donc :

$$|V| = S(P) \pmod p$$

Et tout revient à montrer que $S(P)=0$. L'hypothèse $\sum \deg(f_\alpha) < n$ entraîne :

$$\deg(P) < n(q-1)$$

Donc P est combinaison linéaire de monômes :

$$X^u = {X_1}^{u_1} \dots {X_n}^{u_n}$$

avec $\sum u_i < n(q-1)$. Il suffit alors de prouver que, pour un tel monôme X^u, on a $S(X^u)=0$. Mais cela résulte de lemme précédent, puisque l'un au moins des u_i est inférieur à $q-1$. $\square$

Corollaire 1.1.1. Si $\sum \deg(f_\alpha) < n$ et si les f_α sont sans terme constant, alors les f_α ont un zéro commun non trivial.
Démonstration : Si V était réduit à $\{0\}$, on aurait $|V|=1$ et dans ce cas là $|V| \neq 0 \pmod p$.
$\square$

Corollaire 1.1.2. Toute forme quadratique d'au moins 3 variables sur K a un vecteur isotrope non trivial.
Démonstration : Il suffit d'appliquer le corollaire précédent dans le cas où on considère une seule forme homogène, de degré $2 < 3$. $\square$

1.2 Loi de réciprocité quadratique

1.2.1 Symbole de Legendre

Définition 1.2.1. Soit p un nombre premier impair et $\bar{a} \in \mathbb{F}_p$, on définit le symbole de Legendre :

$$\left(\frac{\bar{a}}{p}\right) := \begin{cases} 0 & \text{si } \bar{a} = \bar{0} \\ 1 & \text{si } \bar{a} \neq \bar{0} \text{ est un carré modulo } p \\ -1 & \text{si } \bar{a} \neq \bar{0} \text{ n'est pas un carré modulo } p \end{cases}$$

Proposition 1.2.1. (*Critère d'Euler*) Pour $\bar{a} \in \mathbb{F}_p^\times$, on a : $\overline{\left(\frac{\bar{a}}{p}\right)} = \bar{a}^{\frac{p-1}{2}}$.

Démonstration : Les carrés modulo p sont exactement les racines dans $\mathbb{F}_p^\times$ de $X^{\frac{p-1}{2}} - 1$. Comme $\mathbb{F}_p^\times$ est d'ordre $p-1$, $\bar{a}^{\frac{p-1}{2}}$ est d'ordre au plus 2, donc

$$\bar{a}^{\frac{p-1}{2}} = \begin{cases} \bar{1} \text{ si } a \text{ est un carré modulo } p \\ \overline{-1} \text{ si } a \text{ n'est pas un carré modulo } p \end{cases} = \overline{\left(\frac{a}{p}\right)}.$$

□

On prolonge le symbole de Legendre aux entiers relatifs en posant pour $a \in \mathbb{Z}$, $\left(\frac{a}{p}\right) := \left(\frac{\bar{a}}{p}\right)$.

Théorème 1.2.1. *Pour $a, b \in \mathbb{Z}$, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ et si p ne divise pas a, $\left(\frac{a}{p}\right)^{-1} = \left(\frac{a}{p}\right)$.*
On a aussi les relations suivantes :

(i) $\left(\frac{1}{p}\right) = 1$;

(ii) $\left(\frac{-1}{p}\right) = \begin{cases} 1 \textit{ si } p = 1 \pmod 4 \\ -1 \textit{ si } p = 3 \pmod 4 \end{cases}$;

(iii) $\left(\frac{2}{p}\right) = \begin{cases} 1 \textit{ si } p = \pm 1 \pmod 8 \\ -1 \textit{ si } p = \pm 5 \pmod 8 \end{cases}$.

Démonstration : La multiplicativité résulte du critère d'Euler et, si p ne divise pas a, alors $\left(\frac{a}{p}\right) \in \{-1; 1\}$ est son propre inverse. De plus, (i) est immédiat et (ii) provient aussi du critère d'Euler. Montrons (iii) ; soit Ω une clôture algébrique de $\mathbb{F}_p$ et $\alpha \in \Omega$ une racine 8-ième de l'unité. On a $\alpha^4 = -1$ et donc $\alpha^2 + \alpha^{-2} = 0$. Posons $y = \alpha + \alpha^{-1}$, alors $y^2 = 2$ et $y^p = \alpha^p + \alpha^{-p}$ (on est en caractéristique p). Si $p = \pm 1 \pmod 8$, alors $y^p = \alpha^{\pm 1} + \alpha^{\mp 1} = y$, donc $2^{\frac{p-1}{2}} = y^{p-1} = 1$. Sinon on a $p = \pm 5 \pmod 8$, donc $y^p = \alpha^{\pm 5} + \alpha^{\mp 5} = \alpha^5 + \alpha^{-5}$. On observe que $1 + \alpha^2 + \alpha^4 + \alpha^6 = 0$ (c'est la somme des racines 4-ièmes de l'unité), donc $\alpha^5(\alpha^5 + \alpha^{-5} + \alpha^1 + \alpha^{-1}) = \alpha^2 + 1 + \alpha^6 + \alpha^4 = 0$. Comme $\alpha^5 \neq 0$, on a $\alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1})$, donc $y^p = -(\alpha + \alpha^{-1}) = -y$, d'où $y^{p-1} = -1$. □

Remarque : On peut reformuler les points (ii) et (iii) en : « -1 est un carré modulo p *ssi* $p = 1 \pmod 4$» et « 2 est un carré modulo p *ssi* $p = \pm 1 \pmod 8$».

1.2.2 Loi de réciprocité quadratique

On consacre cette partie à une propriété fondamentale du symbole de Legendre :

Théorème 1.2.2. *(Loi de réciprocité quadratique) Soient p et q deux nombres premiers impairs et distincts. Alors :*

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

Parmi les (très) nombreuses démonstrations de ce résultat (au moins 196), on en proposera deux. Avant de passer aux preuves, illustrons ce résultat ; la loi de réciprocité quadratique nous dit que $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ sauf si p et q sont simultanément congrus à 3 modulo 4, auquel cas $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. Par exemple, $\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{3}{5}\right) = -1$.

Première démonstration :

Lemme 1.2.1. (*de Gauss*) Soit a un entier non divisible par p. On considère les nombres $a, 2a, \dots \frac{p-1}{2}a$ et on réduit chacun d'entre eux à son représentant le plus petit en valeur absolue, *i.e* au nombre $r_k = ka \pmod p$, où $-\frac{p-1}{2} \leq r_k \leq \frac{p-1}{2}$ pour tout k. Alors, $\left(\frac{a}{p}\right) = (-1)^s$, où s est le nombre de k tels que $r_k < 0$.

Démonstration du lemme : On note $u_1, \dots, u_s$ les représentants < 0 et $v_1, \dots, v_{\frac{p-1}{2}-s}$ ceux ≥ 0.On remarque que les nombres $-u_1, \dots, -u_s$ sont tous compris entre 1 et $\frac{p-1}{2}$, et qu'ils sont tous distincts des v_j (en effet si $-u_i = v_j \pmod p$, alors $p \mid u_i + v_j$. Mais $u_i = k.a \pmod p$ et $v_j = l.a \pmod p$, donc $p \mid (k+l).a$. Comme $a \wedge p = 1$ on a (d'après le lemme... de Gauss !) que $p \mid k+l$, ce qui est impossible car $k+l \leq p-1$). Il suit que $\{-u_1, \dots, -u_s, v_1, \dots, v_{\frac{p-1}{2}-s}\} = \{1, \dots, \frac{p-1}{2}\}$, d'où :

$$(-1)^s \prod_{1\leq i\leq s} u_i \prod_{1\leq j\leq \frac{p-1}{2}} v_j = (\frac{p-1}{2})! \pmod p.$$

En revenant à la définition des u_i et des v_j,

$$(\frac{p-1}{2})! = (-1)^s \prod_{1\leq i\leq s} u_i \prod_{1\leq j\leq \frac{p-1}{2}} v_j = (-1)^s (\frac{p-1}{2})!\ a^{\frac{p-1}{2}} \pmod p.$$

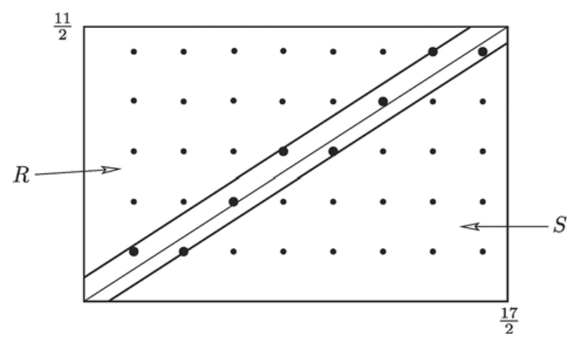
On simplifie par $(\frac{p-1}{2})! \neq 0 \pmod p$ et d'après le critère d'Euler,

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = (-1)^s \pmod p.$$

Comme $-1 \neq 1 \pmod p$, on a bien montré que $\left(\dfrac{a}{p}\right) = (-1)^s$. $\square$

Remarque. Le lemme permet de calculer facilement $\left(\dfrac{2}{p}\right)$; les nombres $2, 4, \ldots, 2\frac{p-1}{2}$ sont tous compris entre 1 et $p-1$. Alors, $s = \left|\{i \mid \frac{p-1}{2} < 2i \leq p-1\}\right| = \frac{p-1}{2} - \left|\{i \mid 2i \leq \frac{p-1}{2}\}\right| = \frac{p-1}{2} - \left\lfloor \frac{p-1}{4} \right\rfloor = \left\lceil \frac{p-1}{4} \right\rceil$ (partie entière par excès). On retrouve bien que 2 est un carré modulo p lorsque $p = 8k \pm 1$.

On peut maintenant passer à la première démonstration, dûe à Gotthold Eisenstein :
Démonstration du théorème : Supposons que kq est un multiple de q qui se réduit modulo p au représentant $r_k < 0$, cela signifie qu'il existe un unique entier j tel que $-\frac{p}{2} < kq - jp < 0$. Comme $0 < k < \frac{p}{2}$, on a $-\frac{p}{2} < \frac{p}{2}(q-1) - jp$ et donc $0 < j < \frac{q}{2}$. En d'autres termes, et d'après le lemme, $\left(\dfrac{q}{p}\right) = (-1)^s$, où s est le nombre de points du réseau constitué des couples (x, y) d'entiers tels que (i) : $0 < py - qx < \frac{p}{2}$, $0 < x < \frac{p}{2}$, $0 < y < \frac{q}{2}$. Par symétrie, $\left(\dfrac{p}{q}\right) = (-1)^t$, où t est le nombre de points du réseau constitué des couples (x, y) d'entiers tels que (ii) : $0 < qx - py < \frac{p}{2}$, $0 < x < \frac{p}{2}$, $0 < y < \frac{q}{2}$. Dans le rectangle de longueur $\frac{p}{2}$ et de largeur $\frac{q}{2}$, on trace la diagonale d'équation $py = qx$ et ses parallèles d'équations (1) : $py - qx = \frac{p}{2}$ et (2) : $qx - py = \frac{q}{2}$. Par exemple pour $p = 11$ et $q = 17$, cela donne :



On termine la démonstration en faisant quelques remarques :

1) Il n'y a pas de points du réseau sur la diagonale ni sur les deux parallèles. En effet, $py = qx$ impliquerait $p|x$ ce qui est impossible car $x < \frac{p}{2}$. Pour les parallèles, $py - qx$ est un entier mais $\frac{p}{2}$ et $\frac{q}{2}$ ne le sont pas.
2) Les points du réseau qui satisfont la condition (i) sont précisément situés dans la bande supérieure (délimitée par (1) et la diagonale) et ceux vérifiant la condition (ii) sont dans la bande inférieure (délimitée par (2) et la diagonale). Ainsi, le nombre de points du réseau que l'on trouve dans les deux bandes est égal à $s + t$.
3) Les parties extérieures R, définie par $py - qx > \frac{p}{2}$ et S, définie par $qx - py > \frac{q}{2}$ contiennent le même nombre de points. En effet, l'application $\varphi : R \to S$, $(x, y) \mapsto (\frac{p+1}{2} - x, \frac{q+1}{2} - y)$ est bien définie : si $(x, y) \in R$, *i.e* $py - qx > \frac{p}{2}$, alors : $q(\frac{p+1}{2} - x) - p(\frac{q+1}{2} - y) = py - qx + \frac{q}{2} - \frac{p}{2} > \frac{q}{2}$. De plus, φ est clairement involutive.

Comme il y a en tout $\frac{p-1}{2} . \frac{q-1}{2}$ points situés dans le rectangle considéré, on en déduit que

$s+t$ et $\frac{p-1}{2}.\frac{q-1}{2}$ sont de même parité. Finalement,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{s+t} = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}.$$

$\square$

Deuxième démonstration : Celle-ci est plus classique et repose sur les sommes de Gauss. Soit F le corps fini à q^{p-1} éléments. C'est un corps fini de caractéristique q, son groupe multiplicatif est d'ordre $q^{p-1}-1$ et cyclique. Le petit théorème de Fermat nous dit que $p \mid q^{p-1}-1$, et donc par les théorèmes de Sylow (ou simplement Cauchy ici), il existe un élément d'ordre p, notons le $\zeta \in F^\times$. Considérons la somme de Gauss :

$$G := \sum_{i\in\mathbb{F}_p} \left(\frac{i}{p}\right) \zeta^i \in F.$$

On va d'abord montrer deux identités sur les sommes de Gauss, dont la loi de réciprocité quadratique résultera immédiatement.

$$G^2 = (-1)^{\frac{p-1}{2}} p. \tag{1}$$

En utilisant la multiplicativité,

$$G^2 = \sum_{i,j\in\mathbb{F}_p} \left(\frac{ij}{p}\right) \zeta^{i+j} = \sum_{k\in\mathbb{F}_p} \zeta^k \Big(\sum_{i\in\mathbb{F}_p} \left(\frac{i(k-i)}{p}\right) \Big), \quad \text{en posant } k = i+j.$$

On remarque que si $i \neq 0$,

$$\begin{aligned} \left(\frac{i(k-i)}{p}\right) &= \left(\frac{-i^2}{p}\right)\left(\frac{1-ki^{-1}}{p}\right) \\ &= (-1)^{\frac{p-1}{2}} \left(\frac{1-ki^{-1}}{p}\right). \end{aligned}$$

Si on pose $C_k = \sum_{i\in\mathbb{F}_p^\times} \left(\frac{1-ki^{-1}}{p}\right)$, on vient de montrer que :

$$(-1)^{\frac{p-1}{2}} G^2 = \sum_{k\in\mathbb{F}_p} C_k \zeta^k.$$

Si $k=0$, $C_0 = \sum_{i\in\mathbb{F}_p^\times} \left(\frac{1}{p}\right) = p-1$; sinon $s = 1-ki^{-1}$ décrit $\mathbb{F}_p\backslash\{1\}$ quand i décrit $\mathbb{F}_p^\times$ (l'inverse est $\mathbb{F}_p\backslash\{1\} \to \mathbb{F}_p^\times$, $s \mapsto k(1-s)^{-1}$) et $C_k = \sum_{s\in\mathbb{F}_p} \left(\frac{s}{p}\right) - \left(\frac{1}{p}\right) = -\left(\frac{1}{p}\right) = -1$, car dans $\mathbb{F}_p^\times$ il y a autant d'éléments qui sont des carrés que d'éléments qui n'en sont pas. Finalement,

$$G^2(-1)^{\frac{p-1}{2}} = \sum_{k\in\mathbb{F}_p} C_k\zeta^k = p-1+\sum_{k\in\mathbb{F}_p^\times}(-\zeta^k) = p-1-\Big(\sum_{k\in\mathbb{F}_p}\zeta^k - 1\Big) = p.$$

En particulier, $G \neq 0$. Montrons maintenant :

$$G^{q-1} = \left(\frac{q}{p}\right). \tag{2}$$

En effet,

$$\begin{aligned}
G^q &= \sum_{i\in\mathbb{F}_p}\left(\frac{i}{p}\right)^q\zeta^{iq}, \quad \text{en appliquant le Frobenius.}\\
&= \sum_{i\in\mathbb{F}_p}\left(\frac{i}{p}\right)\zeta^{iq}, \quad \text{car } \left(\frac{i}{p}\right)^q = \left(\frac{i}{p}\right) (q \text{ est impair}).\\
&= \left(\frac{q}{p}\right)\sum_{i\in\mathbb{F}_p}\left(\frac{qi}{p}\right)\zeta^{iq}, \quad \text{d'après la multiplicativité.}\\
&= \left(\frac{q}{p}\right)G, \quad \text{car } i\mapsto i.q \text{ est une permutation de } \{0,\dots,p-1\}.
\end{aligned}$$

Le résultat s'obtient alors en divisant par G (non nul). On peut maintenant conclure,

$$\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = \left(\frac{G^2}{q}\right) = (G^2)^{\frac{q-1}{2}} = G^{q-1} = \left(\frac{q}{p}\right)$$

Mais, $\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$, donc :

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

□

1.3 Rappels et compléments sur les formes quadratiques

Dans ce paragraphe, K désigne un corps commutatif de caractéristique différente de 2, et V un K-espace vectoriel de dimension finie.

Définition 1.3.1. Une application $q : V \to K$ est une *forme quadratique sur* K (ou un K-forme quadratique) si :

1) Pour tout $a \in K$ et tout $x \in V$, $q(ax) = a^2 q(x)$;
2) L'application $\varphi : (x, y) \mapsto \frac{1}{4}\big(q(x+y) - q(x-y)\big)$ est bilinéaire symétrique, on dira que φ est la *forme polaire* de q.

On dit alors que (V, q) (parfois (V, φ)) est un *espace quadratique.*

Définition 1.3.2. Soient q une forme quadratique et φ sa forme polaire associée, on dit que (V, q) est *non-dégénéré* si φ est non-dégénérée, c'est-à-dire si :

$$V^\perp = \{x \in V \mid (\forall y \in V)\ \varphi(x, y) = 0\} = \{0\}.$$

Définition 1.3.3. Soit q une forme quadratique, on note $C(q)$ le *cône isotrope* de q défini par :

$$C(q) = \{x \in V \mid q(x) = 0\}.$$

Si $x \in C(q)$, on dit alors que x est un *vecteur isotrope.*

Définition 1.3.4. On appelle *plan hyperbolique*, un espace quadratique de dimension 2 engendré par deux vecteurs isotropes x et y tels que $\varphi(x, y) \neq 0$.
Quitte à multiplier y par $\frac{1}{\varphi(x,y)}$, on peut supposer $\varphi(x, y) = 1$ et alors la matrice de la forme quadratique dans la base (x, y) est :

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Définition 1.3.5. Soient (V_1, q_1), (V_2, q_2) deux espaces quadratiques. Une *isométrie* de (V_1, q_1) dans (V_2, q_2) est une application K-linéaire $f : V_1 \to V_2$ telle que pour tout $v \in V_1$:

$$q_2 \circ f(v) = q_1(v)$$

c'est-à-dire que f préserve les formes quadratiques.
Si une telle application existe entre (V_1, q_1) et (V_2, q_2), on dit que les espaces quadratiques sont *isomorphes.*

Proposition 1.3.1. Tout espace quadratique (V, q) admet une base orthogonale.

Théorème 1.3.1. *(Witt, Simplification des espaces quadratiques) Soient* (V_1, q_1)*,* (V_2, q_2) *et* (W, q) *trois espaces quadratiques non-dégénérés tels que* $(V_1 \oplus W, q_1 \oplus q) \simeq (V_2 \oplus W, q_2 \oplus q)$*, alors :*

$$(V_1, q_1) \simeq (V_2, q_2).$$

Démonstration : Nous ne ferons ici qu'une esquisse de la démonstration. Comme W est un espace vectoriel de dimension finie, (W, q) admet une base orthogonale d'après la proposition précédente, il suffit donc de ne traiter que le cas $\dim_K(W) = 1$, *i.e.* $W = Ke$. Ensuite, on peut montrer qu'il existe une isométrie $V_1 \oplus W \to V_2 \oplus W$ qui envoie $\{0_{V_1}\} \oplus W$ sur $\{0_{V_2}\} \oplus W$, elle induit donc une isométrie entre les orthogonaux. $\square$

Théorème 1.3.2. *(Witt, prolongement des isomorphismes) Soient* (V, q) *un espace quadratique non-dégénéré,* W *un sous-*K*-espace vectoriel de* V *et* $f : W \to V$ *une application injective et isométrique (telle que* $q \circ f = q_{|W}$*). Alors* f *se prolonge en une isométrie de* V*.*

Définition 1.3.6. Deux formes quadratiques q_1 et q_2 sur V sont *équivalentes* lorsqu'il existe $u \in \mathrm{GL}(V)$ tel que :

$$q_2 = q_1 \circ u$$

Définition 1.3.7. Soient (V, q) un espace quadratique sur K et φ la forme polaire de q. On dispose de l'application linéaire

$$\ell_q : \left\{ \begin{array}{ccc} V & \to & V^* \\ x & \mapsto & \varphi(x, \cdot) \end{array} \right.$$

On définit le *rang* de q comme le rang de ℓ_q. Notons que si $\mathcal{B} = (e_1, \ldots, e_n)$ est une vase de V sur K, et $\mathcal{B}^*$ la base duale de $\mathcal{B}$, la matrice de q dans $\mathcal{B}$ est la matrice de ℓ_q dans les bases $\mathcal{B}$ et $\mathcal{B}^*$, et le rang de q est égal au rang de cette matrice.

Définition 1.3.8. Soit (V, φ) un espace quadratique. Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base de V, la *matrice de φ dans la base $\mathcal{B}$* est définie par :

$$\mathrm{Mat}_{\mathcal{B}}(\varphi) = \big(\varphi(e_i, e_j)\big)_{1 \leq i,j \leq n} \in \mathcal{M}_n(K).$$

Définition 1.3.9. Soit q une forme quadratique de forme polaire φ et soit $\mathcal{B}$ une base de V sur K, on appelle le *discriminant* de φ l'image de $\det\big(\mathrm{Mat}_{\mathcal{B}}(\varphi)\big)$ dans $\{0\} \cup (K^\times / K^{\times 2})$. On le note $\mathrm{disc}(q)$.

Définition 1.3.10. On suppose que $K = \mathbb{R}$. La *signature* d'une forme quadratique q est le couple (s, t) où s (respectivement t) est la plus grande des dimensions des sous-espaces E de V tels que la restriction $q_{|E}$ de q à E soit définie positive (respectivement définie négative).

Définition 1.3.11. Soit (V, q) un espace quadratique. Le *noyau* de la forme quadratique q est $V^\perp$.
De plus, si W est un complémentaire de $V^\perp$, alors $q_{|W}$ est non-dégénérée et $(V, q) = (V^\perp, 0) \overset{\perp}{\oplus} (W, q_{|W})$. On remarque alors que pour classifier les espaces quadratiques sur un corps K, il suffit de classifier ceux qui sont non-dégénérés.

Le but de ce mémoire est de classifier les formes quadratiques sur le corps des rationnels $\mathbb{Q}$. Classifier les formes quadratiques sur un corps K revient à déterminer les classes d'isomorphismes des espaces quadratiques sur K. On sait déjà le faire pour certains corps K. Voici quelques exemples :

1) Si K est un corps algébriquement clos (par exemple $\mathbb{C}$), un espace quadratique est entièrement déterminé par sa dimension et son rang (à isomorphisme près).

2) Lorsque $K = \mathbb{R}$, un espace quadratique est déterminé par sa dimension, son rang et sa signature (grâce au théorème d'inertie de Sylvester).

3) Lorsque K est un corps fini (par exemple $\mathbb{F}_p$), un espace quadratique est déterminé par sa dimension, son rang et son discriminant.

Définition 1.3.12. Deux bases orthognales $e = (e_1, \ldots, e_n)$ et $e' = (e'_1, \ldots, e'_n)$ de V sont *contiguës* si elles ont un élément en commun (*i.e.* il existe i et j tels que $e_i = e'_j$).

Théorème 1.3.3. *Supposons V non dégénéré de dimension au-moins 3 et soient $e = (e_1, \ldots, e_n)$ et $e' = (e'_1, \ldots, e'_n)$ deux bases orthogonales de V. Il existe une suite finie $e^{(0)}$, $e^{(1)}, \ldots, e^{(m)}$ de bases orthogonales de V telle que $e^{(0)} = e$, $e^{(m)} = e'$, et que $e^{(i)}$ soit contiguë à $e^{(i+1)}$ pour $0 \leq i < m$.*
On dit alors que $e^{(0)}, \ldots, e^{(m)}$ est une chaîne de bases orthogonales contiguës reliant e à e'.

Démonstration : Nous allons distinguer trois cas.
1) Supposons tout d'abord que $\varphi(e_1, e_1) \cdot \varphi(e'_1, e'_1) - \varphi(e_1, e'_1)^2 \neq 0$. Cela revient à dire que e_1 et e'_1 ne sont pas colinéaires et que le plan $P = Ke_1 + Ke'_1$ est non-dégénéré. Il existe alors $\varepsilon_2, \varepsilon'_2 \in P$ tels que :

$$P = Ke_1 \overset{\perp}{\oplus} K\varepsilon_2 \quad \text{et} \quad P = Ke'_1 \overset{\perp}{\oplus} K\varepsilon'_2$$

Notons H l'orthogonal de P ; comme P est non-dégénéré, on a $V = H \overset{\perp}{\oplus} P$. Soit $(e''_3, \ldots, e''_n)$ une base orthogonale de H. On peut alors relier e à e' avec la chaîne :

$$e \to (e_1, \varepsilon_2, e''_3, \ldots, e''_n) \to (e'_1, \varepsilon'_2, e''_3, \ldots, e''_n) \to e''.$$

Ce qui montre le théorème pour le premier cas.
2) Supposons maintenant que l'on ait $\varphi(e_1, e_1) \cdot \varphi(e'_2, e'_2) - \varphi(e_1, e'_2)^2 \neq 0$. On peut alors se ramener au cas précédent en remplaçant e'_1 par e'_2.
3) Supposons finalement que l'on ait $\varphi(e_1, e_1) \cdot \varphi(e'_i, e'_i) - \varphi(e_1; e'_i)^2 = 0$ pour $i = 1$ et 2. Nous allons commencer par démontrer le lemme suivant :

Lemme 1.3.1. Il existe $x \in K$ tel que $e_x = e'_1 + xe'_2$ soit non-isotrope, et engendre avec e_1 un plan non-dégénéré.

Démonstration : On a $\varphi(e_x, e_x) = \varphi(e'_1, e'_1) + x^2\varphi(e'_2, e'_2)$; on doit donc prendre x^2 distinct de $-\frac{\varphi(e'_1, e'_1)}{\varphi(e'_2, e'_2)}$. D'autre part, pour que e_x engendre avec e_1 un plan non-dégénéré, il faut et il suffit que :

$$\varphi(e_1, e_1) \cdot \varphi(e_x, e_x) - \varphi(e_1, e_x)^2 \neq 0$$

Si l'on explicite en tenant compte de l'hypothèse (de notre cas 3)), on trouve que le premier membre est $-2x\varphi(e_1, e'_1) \cdot \varphi(e_1, e'_2)$. Or notre hypothèse 3) implique que $e_1 \cdot e'_1 \neq 0$ pour $i = 1$ et 2. On voit donc que e_x vérifie les conditions du lemme si et seulement si on a à la fois $x \neq 0$ et $x^2 \neq -\frac{\varphi(e'_1, e'_1)}{\varphi(e'_2, e'_2)}$. Cela élimine au plus trois valeurs de x ; si K a au moins 4 éléments, on peut donc trouver un tel x. Reste le cas où $K = \mathbb{F}_3$ (on rappelle que la caractéristique de K est différente de 2, donc le cas $K = \mathbb{F}_2$ est exclu). Dans ce cas tout carré non-nul est égal à 1, et notre hypothèse 3) s'écrit $\varphi(e_1, e_1) \cdot \varphi(e'_i, e'_i) = 1$ pour $i = 1$ et 2 ; le rapport $\frac{\varphi(e'_1, e'_1)}{\varphi(e'_2, e'_2)}$ est donc égal à 1, et, pour réaliser la condition $x^2 \neq 0, -1$, il suffit de prendre $x = 1$. □

Choisissons $e_x = e'_1 + xe'_2$ vérifiant les conditions du lemme. Comme e_x n'est pas isotrope, il existe e''_2 tel que (e_x, e''_2) soit une base orthogonale de $Ke'_1 \overset{\perp}{\oplus} Ke'_2$. On pose alors $e'' = (e_x, e''_2, e'_3, \ldots, e'_n)$, c'est une base orthogonale de V. Comme $Ke_1 + Ke_2$ est un plan non-dégénéré, on utilise la première partie de la démonstration pour montrer que l'on peut relier e à e'' par une chaîne de bases contiguës ; d'autre part e' et e'' sont contiguës. $\square$

Définition 1.3.13. Deux formes quadratiques q et q' sur un espace vectoriel V sont dites *équivalentes* si les espaces quadratiques correspondants sont isomorphes. On écrit alors $q \sim q'$. Si M et M' sont respectivement les matrices de q et de q' dans une base de V, alors $q \sim q'$ revient à écrire $M' = XM^tX$, où X est une matrice inversible.

Définition 1.3.14. Une forme $q(X_1, X_2)$ à deux variables est dite hyperbolique si :

$$q \sim X_1X_2 \sim {X_1}^2 - {X_2}^2.$$

Définition 1.3.15. On dit qu'une forme $q(X_1, \ldots, X_n)$ *représente* un élément a de K s'il existe $x \in K^n$ non-nul tel que $q(x) = a$.

On remarque que q représente 0 si et seulement si l'espace quadratique correspondant contient un vecteur isotrope non-nul.

Proposition 1.3.2. Si q représente 0 et est non-dégénérée, on a $q \sim q_2 + g$ où q_2 est hyperbolique, g non-dégénérée. De plus, q représente tout élément de K.

Corollaire 1.3.1. Soit $q = q(X_1, \ldots, X_{n-1})$ une forme quadratique non-dégénérée, et soit $a \in K^\times$. Les assertions suivantes sont équivalentes :

1) q représente a ;
2) On a $q \sim h + aZ^2$, où h est une forme en $n-2$ variables ;
3) La forme $q' = q - aZ^2$ représente 0.

Démonstration : L'implication 2) $\implies$ 1) est immédiate. Réciproquement, si q représente a, l'espace quadratique V correspondant à q contient un élément x tel que $q(x) = a$. Si H désigne l'orthogonal de x, on a $K^{n-1} = H \overset{\perp}{\oplus} Kx$ et on a bien alors $q \sim h + aZ^2$ où h désigne la forme quadratique attachée à une base de H.
L'implication 2) $\implies$ 3) est elle aussi immédiate. Inversement, si $q' = q - aZ^2$ a un zéro non-trivial $(x_1, \ldots, x_{n-1}, z)$, on a soit $z = 0$, dans ce cas là q représente 0 et donc aussi a ; soit $z \neq 0$, alors :

$$q\left(\frac{x_1}{z}, \ldots, \frac{x_{n-1}}{z}\right) = a.$$

Ce qui montre l'implication et termine la preuve du corollaire. $\square$

Corollaire 1.3.2. Soient g et h deux formes non-dégénérées de rang au moins 1, et soit $f = g - h$. On a équivalence entre :

1) f représente 0 ;
2) Il existe $a \in K^\times$ qui est représenté par g et par h ;
3) Il existe $a \in K^\times$ tel que $q - aZ^2$ et $h - aZ^2$ représentent 0.

Démonstration : Le corollaire précédent permet déjà de prouver l'équivalence entre 2) et 3). L'implication 2) $\implies$ 3) est triviale.
Montrons 1) $\implies$ 2), soit (x, y) un zéro non-trivial de f avec $g(x) = h(y)$. Si $a = g(x) = h(y)$ est non-nul, alors 2) est vérifiée. Si $a = 0$, l'une des formes représente 0 (par symétrie on peut supposer que ceci s'applique à g), donc tout élément de K, et en particulier toute valeur non-nulle prise par l'autre forme (par symétrie, h ici). $\square$

Théorème 1.3.4. *Soit q une forme quadratique en n variables. Alors il existe $a_1, \dots, a_n$ des éléments de K tels que :*

$$q \sim a_1 {X_1}^2 + \cdots + a_n {X_n}^2.$$

Démonstration : Cela provient de l'existence d'une base orthogonale. $\square$

Théorème 1.3.5. *Soient $q = g + h$ et $q' = g' + h'$ deux formes quadratiques non-dégénérées. Si $q \sim q'$ et $g \sim g'$, alors $h \sim h'$.*

Démonstration : C'est une reformulation du théorème de simplification de Witt. $\square$

Corollaire 1.3.3. Si q est non-dégénérée, alors :

$$q \sim q_1 + \cdots + q_m + h$$

où $q_1, \dots, q_m$ sont hyperboliques, et h ne représente pas 0. Cette décomposition est unique, à équivalence près. Le nombre m de facteurs hyperboliques peut être caractérisé comme la dimension des sous-espaces isotropes maximaux de l'espace quadratique correspondant à q.

Terminons ce paragraphe par deux résultats sur les formes quadratiques sur $\mathbb{F}_q$ où $q = p^f$, avec $p \neq 2$ un nombre premier (et $f \neq 0$ bien-sûr).

Proposition 1.3.3. Une forme quadratique sur $\mathbb{F}_q$ de rang au moins 2 (respectivement au moins 3) représente tout élément de $\mathbb{F}_q^\times$ (respectivement de $\mathbb{F}_q$).

Démonstration : D'après le corollaire 1.3.1, il suffit de montrer que toute forme quadratique à 3 variables représente 0. Il s'agit donc de montrer que si $a, b, c \in \mathbb{F}_q$ sont non-nuls, l'équation :

$$ax^2 + by^2 = c \quad (*)$$

a une solution. Notons A l'ensemble des éléments de $\mathbb{F}_q$ de la forme ax^2 et B celui de la forme $c - by^2$ avec x et y dans $\mathbb{F}_q$. Les deux ensembles ont un cardinal de $\frac{q+1}{2}$ on a donc $A \cap B \neq \emptyset$ et $(*)$ a une solution. $\square$

Proposition 1.3.4. Toute forme quadratique non-dégénérée de rang n sur $\mathbb{F}_q$ est équivalente à :

$${X_1}^2 + \cdots + {X_{n-1}}^2 + {X_n}^2 \quad \text{ou} \quad {X_1}^2 + \cdots + {X_{n-1}}^2 + a{X_n}^2$$

avec $a \in \mathbb{F}_q$ non-carré, suivant que son discriminant est ou non un carré.

Démonstration : Le cas $n = 1$ est trivial. Si $n \geq 2$, on utilise la proposition 1.3.3 qui nous permet de dire qu'une forme quadratique f représente 1. Elle est donc équivalente à ${X_1}^2 + g$ où g est une forme à $n - 1$ variables, et par une récurrence on obtient le résultat. $\square$

Remarque : Ces deux résultats justifient la classification des formes quadratiques sur les corps finis $\mathbb{F}_q$.

2 Les nombres p-adiques, les constructions des corps p-adiques

2.1 Construction analytique des corps p-adiques

Définition 2.1.1. Soit $a \in \mathbb{N} \setminus \{0\}$, soit p un nombre premier, on appelle *valuation p-adique* de a et on note $v_p(a)$, le plus grand $m \in \mathbb{N}$ tel que $a = 0 \pmod{p^m}$. Par convention, on posera $v_p(0) = +\infty$.

Proposition 2.1.1. Si $a, b \in \mathbb{Z}^\times$, alors :

$$v_p(ab) = v_p(a) + v_p(b) \qquad v_p(a+b) \geq \min\big(v_p(a), v_p(b)\big)$$

On peut étendre la valuation p-adique à $\mathbb{Q}$ telle que pour tout $x = \frac{a}{b} \in \mathbb{Q}$:

$$v_p\left(x\right) = v_p(a) - v_p(b)$$

On remarque que la dernière écriture ne dépend pas du choix du représentant.

Définition 2.1.2. A partir de cette valuation p-adique, on peut définir une application $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_+$ telle que :

$$x \mapsto \begin{cases} \frac{1}{p^{v_p(x)}} & \text{si} \quad x \neq 0 \\ 0 & \text{si} \quad x = 0 \end{cases}$$

Exemple : Prenons $x = \frac{196}{3} \in \mathbb{Q}$, on peut écrire 196 comme $2^2 \times 7^2$ et on a alors :

$$|x|_7 = \frac{1}{7^{v_7(x)}} = \frac{1}{7^2} = \frac{1}{49}, \qquad |x|_2 = \frac{1}{2^2} = \frac{1}{4}, \qquad |x|_{11} = \frac{1}{11^{v_{11}(x)}} = \frac{1}{11^0} = 1 \qquad |x|_3 = \frac{1}{3^{-1}} = 3$$

Définition 2.1.3. Soit F un corps quelconque $|\cdot| : F \to \mathbb{R}_+$ est une *valeur absolue* si :

- $|x| = x$ si $x > 0$, $|x| = -x$ si $x < 0$ et $|x| = 0$ si $x = 0$;
- $|\cdot|$ vérifie l'inégalité triangulaire : $|x + y| \leq |x| + |y|$;
- $|\cdot|$ est multiplicative : $|xy| = |x| \cdot |y|$.

De plus, $|\cdot|$ est une valeur absolue non-archimédienne (ou ultra-métrique) si c'est une valeur absolue et si :

$$|x + y| \leq \max(|x|, |y|)$$

Exemple : Soit F un corps quelconque, on définit la valeur absolue triviale $|\cdot|_0 \to \mathbb{R}_+$ par :

$$|0|_0 = 0 \quad \text{et} \quad (\forall x \in F,\ x \neq 0)\ |x|_0 = 1$$

Proposition 2.1.2. $|\cdot|_p$ est une valeur absolue sur $\mathbb{Q}$, on l'appellera la *valeur absolue p-adique.*

Démonstration : Vérifions les trois axiomes de la valeur absolue : soit $x \in \mathbb{Q}$, il est déjà immédiat que si $x = 0$ alors $|x|_p = 0$; et si $|x|_p = 0$, alors $v_p(x) = +\infty$ et $x = 0$. Soit $y \in \mathbb{Q}$, alors :

$$|xy|_p = \frac{1}{p^{v_p(xy)}} = \frac{1}{p^{v_p(x)}}\frac{1}{p^{v_p(y)}} = |x|_p|y|_p$$

Il nous reste plus qu'à vérifier l'inégalité triangulaire, si x et y sont tous deux non-nuls, alors :

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

On obtient alors :

$$|x+y|_p = \frac{1}{p^{v_p(x+y)}} \leq \max\left(p^{-v_p(x)}, p^{-v_p(y)}\right) = \max(|x|_p, |y|_p) \leq |x|_p + |y|_p$$

Donc $|\cdot|_p$ est bien une valeur absolue. $\square$

Proposition 2.1.3. Soit $|\cdot|$ une valeur absolue ultra-métrique sur un corps K de caractéristique 0 ($e.g$ $\mathbb{Q}$) ; notons A l'image de $\mathbb{Z}$ dans K, alors :

(i) Si $x \in A$, alors $|x| \leq 1$;

(ii) Si $x, y \in K$ tels que $|x| \neq |y|$ alors $|x+y| = \max(|x|, |y|)$;

(iii) En notant pour $x, y \in K$, $\mathrm{d}(x,y) = |x-y|$, si $x, y, z \in K$ alors $\mathrm{d}(x,y) \leq \max(\mathrm{d}(x,z), \mathrm{d}(z,y))$.

Démonstration : (i) Comme $|\pm 1| = 1$, on a $|a \pm 1| \leq \max(|a|, 1)$, par une récurrence immédiate, cela implique que $|a| \leq 1$.
(ii) Quitte à échanger x et y, on peut supposer $|x| > |y|$, alors :

$$|x+y| \leq |x| = \max(|x|, |y|)$$

D'autre part, on peut écrire x comme : $x = (x+y) - y$, alors :

$$|x| \leq \max(|x+y|, |y|)$$

Or comme on a supposé $|x| > |y|$, cette inégalité n'est vraie que si $\max(|x+y|, |y|) = |x+y|$. Et on obtient alors : $|x| \leq |x+y|$. Donc :

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

(iii) Il suffit d'appliquer la condition ultra-métrique de la valeur absolue à $x - y = (x-z) + (z-y)$. $\square$

Remarque : La valeur absolue $|\cdot|_p$ est ultra-métrique.

La valeur absolue p-adique induit alors une distance sur $\mathbb{Q}$, donc induit une topologie dont une base d'ouvert est formée des boules ouvertes définies par :

$$\mathcal{B}(a,r) = \{x \in \mathbb{Q} \mid |x-a|_p < r\}$$

Nous disposons d'une propriété (étonnante) sur ces boules ouvertes :

Proposition 2.1.4. Soient $a \in \mathbb{Q}$, $r > 0$, on note $\mathcal{B}(a,r)$ la boule centrée en a de rayon r pour la valeur absolue $|\cdot|_p$. Si $b \in \mathcal{B}(a,r)$ alors $\mathcal{B}(a,r) = \mathcal{B}(b,r)$, *i.e.* tout point contenu dans une boule est le centre de cette boule.

Démonstration : Soit $b \in \mathcal{B}(a,r)$ alors $|b-a|_p < r$. Prenons maintenant $x \in \mathcal{B}(a,r)$ alors, comme $|\cdot|_p$ est ultra-métrique :

$$|x-b|_p \leq \max\left(|x-a|_p, |b-a|_p\right) < r$$

Donc $x \in \mathcal{B}(b,r)$ et on a l'inclusion $\mathcal{B}(a,r) \subset \mathcal{B}(b,r)$. L'inclusion réciproque s'obtient par symétrie. $\square$

Remarque : Cette proposition reste vraie pour toute valeur absolue ultra-métrique, pas seulement pour $|\cdot|_p$.

Théorème 2.1.1. *(Ostrowski-1916) Toute valeur absolue non-triviale sur $\mathbb{Q}$ est équivalente à $|\cdot|_p$ pour p premier ou $p = \infty$ (la valeur absolue usuelle $|\cdot|_\infty$).*

Commençons par rappeler que deux valeurs absolues sur un corps K sont équivalentes si elles définissent la même topologie sur K et montrons le lemme suivant :

Lemme 2.1.1. *Deux valeur absolue $|\cdot|_1$ et $|\cdot|_2$ sont équivalentes s'il existe un réel $\alpha > 0$ tel que :*

$$|x|_1 = |x|_2^\alpha \quad (\forall x \in K)$$

Démonstration du lemme : Supposons qu'un tel réel α existe, alors, pour x et a dans K :

$$|x-a|_1 < r \iff |x-a|_2^\alpha < r \iff |x-a|_2 < r^{1/\alpha}$$

Ainsi, toute boule ouverte pour la valeur absolue $|\cdot|_1$ reste une boule ouverte pour la valeur absolue $|\cdot|_2$ mais de rayon différent. Cela suffit pour montrer que les topologies définies par les deux valeurs absolues sont identiques et qu'elles sont donc équivalentes. $\square$

Démonstration du théorème d'Ostrowski : Notons $|\cdot|$ une telle valeur absolue non-triviale sur $\mathbb{Q}$.
On distinguera deux cas :
•Premier cas : supposons que $|\cdot|$ est une valeur absolue archimédienne. Nous voulons montrer que dans ce cas là, $|\cdot|$ est équivalente à la valeur absolue usuelle $|\cdot|_\infty$. Posons n_0 le plus petit entier tel que $|n_0| > 1$ (son existence est assurée car la valeur absolue est archimédienne). On peut alors définir le réel positif α tel que :

$$|n_0| = {n_0}^\alpha$$

Ce α va nous permettre de réaliser l'équivalence entre $|\cdot|$ et $|\cdot|_\infty$. Il faut alors prouver que pour tout $x \in \mathbb{Q}$, on a $|x| = {|x|_\infty}^\alpha$. On sait que cette égalité est vraie pour n_0, montrons alors qu'elle est vraie pour tout $n \in \mathbb{Z}$. Pour ce faire, écrivons n en base n_0, alors :

$$n = a_0 + a_1 n_0 + \cdots + a_k {n_0}^k$$

Avec $0 \leq a_i \leq n_0 - 1$ et $a_k \neq 0$. Remarquons déjà que k est déterminé par l'inégalité ${n_0}^k \leq n < {n_0}^{k+1}$, ce qui nous dit que :

$$k = \left\lfloor \frac{\log n}{\log n_0} \right\rfloor$$

En notant $\lfloor x \rfloor$ la partie entière de x. Prenons maintenant la valeur absolue, on obtient ainsi :

$$\begin{aligned} |n| &= |a_0 + a_1 n_0 + \cdots a_k {n_0}^k| \\ &\leq |a_0| + |a_1| {n_0}^\alpha + \cdots + |a_k| {n_0}^{k\alpha} \end{aligned}$$

Comme on a pris n_0 comme le plus petit entier tel que $|n_0| > 1$, on sait que $|a_i| \leq 1$ et on obtient :

$$\begin{aligned} |n| &\leq 1 + {n_0}^\alpha + \cdots + {n_0}^{k\alpha} \\ &= {n_0}^{k\alpha}(1 + {n_0}^{-\alpha} + \cdots + {n_0}^{-k\alpha}) \\ &\leq {n_0}^{k\alpha} \sum_{i \geq 0} {n_0}^{-i\alpha} = {n_0}^{k\alpha} \frac{{n_0}^\alpha}{{n_0}^\alpha - 1} \end{aligned}$$

Posons $C = \frac{{n_0}^\alpha}{{n_0}^\alpha - 1}$ (qui est d'ailleurs positif), l'équation du dessus peut alors s'écrire :

$$|n| \leq C {n_0}^{k\alpha} \leq C n^\alpha$$

Cette formule est vraie pour tout n, on peut donc l'appliquer à n^N, pour $N \in \mathbb{N}^*$, ce qui nous donne :

$$|n^N| \leq C n^{N\alpha}$$

Comme $C > 0$, on peut prendre la racine N-ième, alors :

$$|n| \leq \sqrt[N]{C} n^\alpha$$

Ceci est vrai pour tout N, on peut faire tendre $N \to +\infty$, ce qui donne $\sqrt[N]{C} \to 1$, et l'inégalité $|n| \leq n^\alpha$. Montrons maintenant l'inégalité inverse pour avoir égalité.
Reprenons l'expression de n en base n_0 :

$$n = a_0 + a_1 n_0 + \cdots + a_k {n_0}^k$$

Comme ${n_0}^{k+1} > n \geq {n_0}^k$, on obtient :

$${n_0}^{(k+1)\alpha} = |{n_0}^{k+1}| = |n + {n_0}^{k+1} - n| \leq |n| + |{n_0}^{k+1} - n|$$

Tel qu'on ait :

$$|n| \geq {n_0}^{(k+1)\alpha} - |{n_0}^{k+1} - n| \geq {n_0}^{(k+1)\alpha} - ({n_0}^{k+1} - n)^\alpha$$

On peut maintenant utiliser l'inégalité obtenue précédemment. Comme $n \geq {n_0}^k$, il suit que :

$$\begin{aligned} |n| &\geq {n_0}^{(k+1)\alpha} - ({n_0}^{k+1} - {n_0}^k)^\alpha \\ &= {n_0}^{(k+1)\alpha} \left(1 - \left(1 - \frac{1}{n_0}\right)^\alpha\right) \\ &= C' {n_0}^{(k+1)\alpha} > C' n^\alpha \end{aligned}$$

Avec ici $C' = 1 - \left(1 - \frac{1}{n_0}\right)^\alpha$ qui ne dépend pas de n et qui est positif. En procédant de même que précédemment, on montre que $|n| \geq n^\alpha$ et donc $|n| = n^\alpha$ pour tout entier n, et d'après les propriétés de la valeur absolue, ceci reste vrai pour tout $x \in \mathbb{Q}$. On vient donc de montrer que $\|\cdot\|$ est équivalente à la valeur absolue usuelle sur $\mathbb{Q}$: $|\cdot|_\infty$.
•Deuxième cas : Supposons désormais que $\|\cdot\|$ est ultra-métrique (non-archimédienne). On sait alors que pour tout entier n, on a $|n| \leq 1$. Comme $\|\cdot\|$ est non-triviale, il existe n_0 le plus petit entier tel que $|n_0| < 1$. La première chose que l'on remarque est que n_0 doit être un premier, puisque sinon $n_0 = a \times b$ avec a et b strictement inférieurs à n_0, puis, par minimalité de n_0, on aurait $|a| = |b| = 1$ et donc $|n_0| = 1$, contradiction. On a donc un nombre premier, notons-le p. On veut maintenant montrer que $\|\cdot\|$ est équivalente à la valeur absolue p-adique (avec p choisi juste avant).
Montrons maintenant que si $n \in \mathbb{Z}$, non divisible par p, alors $|n| = 1$. Soit donc un tel n. Ecrivons la division euclidienne de n par p :

$$n = pr + s$$

avec $0 < s < p$. Par minimalité de p, on a $|s| = 1$; on a aussi $|rp| < 1$ puisque $|r| \leq 1$. Comme $\|\cdot\|$ est non-archimédienne, il suit que $|n| = 1$.
Finalement, pour tout $n \in \mathbb{Z}$, on peut écrire n comme $p^{v_p(n)} n'$ avec $p \nmid n'$. Alors :

$$|n| = |p|^{v_p(n)} |n'| = |p|^{v_p(n)} = c^{-v_p(n)}$$

Où $c = |p|^{-1} > 1$, donc $\|\cdot\|$ est équivalente à la valeur absolue p-adique $|\cdot|_p$. □

Proposition 2.1.5. (La formule du produit) Soit $x \in \mathbb{Q}^\times$, on a :

$$\prod_{p \leq \infty} |x|_p = 1$$

Où $p \leq \infty$ signifie que le produit est sur tous les nombres premiers y compris "celui infini".

Démonstration : Il suffit de montrer la proposition dans le cas où $x \in \mathbb{N}^*$, le cas général en découlera. Soit donc x un entier positif. On peut écrire x en produit de facteurs premiers :

$$x = {p_1}^{\alpha_1} ... {p_n}^{\alpha_n}$$

On a alors :

$$\begin{cases} |x|_q &= 1 & \text{si} \quad q \neq p_i \\ |x|_{p_i} &= p_i^{-\alpha_i} & \text{si} \quad i = 1, 2, ..., n \\ |x|_\infty &= {p_1}^{\alpha_1} ... {p_n}^{\alpha_n} & \end{cases}$$

On obtient le résultat en effectuant le produit. □

Fixons pour la suite un nombre premier $p \neq \infty$. On rappelle qu'une suite $(a_n)_\mathbb{N}$ est de Cauchy si :

$$(\forall \varepsilon > 0)(\exists N \in \mathbb{N}), (\forall n, m \geq N) : |a_n - a_m| < \varepsilon$$

Munissons $\mathbb{Q}$ de la valeur absolue p-adique $|\cdot|_p$.

Lemme 2.1.2. Une suite rationnelle $(x_n)_{\mathbb{N}}$ est de Cauchy par rapport à la valeur absolue p-adique $|\cdot|_p$ si et seulement si :

$$\lim_{n\to+\infty} |x_{n+1} - x_n|_p = 0$$

Démonstration : Soit $(x_n)_{\mathbb{N}}$ une suite telle que $\lim\limits_{n\to\infty} |x_{n+1} - x_n|_p = 0$. Prenons $m = n + r > n$, on obtient :

$$\begin{array}{rcl} |x_m - x_n|_p & = & |x_{n+r} - x_{n+r-1} + x_{n+r-1} - x_{n+r-2} + \cdots + x_{n+1} - x_n|_p \\ & \leq & \max\left(|x_{n+r} - x_{n+r-1}|_p, ..., |x_{n+1} - x_n|_p\right) \end{array}$$

En passant alors à la limite, on voit que la suite est de Cauchy. La réciproque est immédiate.
□

Remarque : Pour n'importe quelle valeur absolue non-triviale $\mathbb{Q}$ n'est pas complet.

Définition 2.1.4. Notons $\mathfrak{C}_p$ l'ensemble des suites de Cauchy de $\mathbb{Q}$ pour la valeur absolue p-adique, *i.e.* :

$$\mathfrak{C}_p = \{(x_n)_{\mathbb{N}} \text{ de Cauchy par rapport à } |\cdot|_p\}$$

Dans la suite, on notera $\mathfrak{C}$ au lieu de $\mathfrak{C}_p$.

Proposition 2.1.6. $\mathfrak{C}$ est un anneau unitaire commutatif. On a :

$$(x_n)_{\mathbb{N}} + (y_n)_{\mathbb{N}} = (x_n + y_n)_{\mathbb{N}} \quad \text{et} \quad (x_n)_{\mathbb{N}} \cdot (y_n)_{\mathbb{N}} = (x_n y_n)_{\mathbb{N}}$$

Lemme 2.1.3. On dispose de l'application :

$$\left\{ \begin{array}{ccc} \mathbb{Q} & \hookrightarrow & \mathfrak{C} \\ x & \mapsto & (x) = (x, x, ...) \end{array} \right.$$

Définition 2.1.5. Notons $\mathcal{N} \subset \mathfrak{C}$ l'idéal :

$$\mathcal{N} := \{(x_n)_{\mathbb{N}} \mid \lim_{n\to+\infty} |x_n|_p = 0\}$$

Lemme 2.1.4. $\mathcal{N}$ est un idéal maximal de $\mathfrak{C}$.

Démonstration : Soit $x = (x_n)_{\mathbb{N}} \in \mathfrak{C}$ ne tendant pas vers 0, notons I l'idéal engendré pas x et $\mathcal{N}$. Montrons alors que I est en fait $\mathfrak{C}$ tout entier, pour ce faire, nous allons montrer que (1) est dans I.
Etant donné que x ne tend pas vers 0, il existe $c > 0$ et $N \in \mathbb{N}$ tels que dès que $n \geq N$, $|x_n|_p \geq c$. On peut alors définir une suite $(y_n)_{\mathbb{N}}$ telle que :

$$\left\{ \begin{array}{lll} y_n = 0 & \text{si} & n < N \\ y_n = \frac{1}{x_n} & \text{si} & n \geq N \end{array} \right.$$

Il est immédiat que $(y_n)_{\mathbb{N}}$ est une suite de Cauchy puisque si $n \geq N$, alors :

$$|y_{n+1} - y_n|_p = \left| \frac{1}{x_{n+1}} - \frac{1}{x_n} \right|_p = \frac{|x_{n+1} - x_n|_p}{|x_n x_{n+1}|_p} \leq \frac{|x_{n+1} - x_n|_p}{c^2} \longrightarrow 0$$

Donc $(y_n)_{\mathbb{N}} \in \mathfrak{C}$. On remarque alors que :

$$x_n y_n = \begin{cases} 0 & \text{si} \quad n < N \\ 1 & \text{si} \quad n \geq N \end{cases}$$

Ce qui signifie que la suite $(x_n y_n)_{\mathbb{N}}$ contient un nombre fini de 0 et une infinité de 1. En particulier, si on considère la suite $(1) - (x_n y_n)_{\mathbb{N}}$, on obtient une suite qui tend vers 0 en l'infini. On a alors :

$$(1) - (x_n)_{\mathbb{N}}(y_n)_{\mathbb{N}} \in \mathcal{N}$$

Or, cela signifie que (1) peut s'écrire comme un multiple de (x_n) plus un élément de $\mathcal{N}$, ce qui veut dire que cette suite est dans I. $\square$

Définition 2.1.6. On définit le corps p-adique comme étant le quotient de l'anneau $\mathfrak{C}$ et de son idéal maximal $\mathcal{N}$:

$$\mathbb{Q}_p = \mathfrak{C}/\mathcal{N}$$

On peut aussi définir $\mathbb{Q}_p$ comme le complété de $\mathbb{Q}$ pour la valeur absolue p-adique $|\cdot|_p$.

Lemme 2.1.5. Soit $(x_n)_{\mathbb{N}} \in \mathfrak{C}$, $(x_n)_{\mathbb{N}} \notin \mathcal{N}$. La suite réelle $(|x_n|_p)$ est stationnaire.

Démonstration : Comme $(x_n)_{\mathbb{N}}$ est une suite de Cauchy ne tendant pas vers zéro, il existe c et N_1 tels que pour tout $n \geq N_1$:

$$|x_n|_p \geq c > 0$$

Par ailleurs, il existe aussi N_2 tel que pour tout $n, m \geq N_2$:

$$|x_n - x_m|_p < c$$

Posons alors $N := \max\{N_1, N_2\}$, on a alors pour tout $n, m \geq N$:

$$|x_n - x_m|_p \leq \max\{|x_n|_p, |x_m|_p\}$$

Alors, par la propriété non-archimédienne de la valeur absolue p-adique : $|x_n|_p = |x_m|_p$. $\square$

Définition 2.1.7. Si λ est un élément de $\mathbb{Q}_p$, et $(x_n)_{\mathbb{N}}$ une suite de Cauchy représentant λ, alors on définit :

$$|\lambda|_p = \lim_{n \to +\infty} |x_n|_p$$

L'existence de la limite est assurée par le lemme précédent.

Proposition 2.1.7. L'image de $\mathbb{Q}$ par l'inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ est dense dans $\mathbb{Q}_p$.

Démonstration : Nous allons montrer que toute boule ouverte autour d'un élément $\lambda \in \mathbb{Q}_p$ contient un élément de (l'image de) $\mathbb{Q}$, *i.e.*, une suite constante. Commençons par fixer $\varepsilon > 0$

le rayon de la boule. Nous allons montrer qu'il y a une suite constante dans la boule ouverte $\mathcal{B}(\lambda, \varepsilon)$.
Premièrement, prenons $(x_n)_{\mathbb{N}}$ une suite de Cauchy représentant λ et soit $\varepsilon' < \varepsilon$, il existe un rang N tel que pour tout $n, m \geq N$, on ait : $|x_n - x_m|_p < \varepsilon'$. Posons $y = x_N$ et considérons la suite constante (y). On peut déjà affirmer que $(y) \in \mathcal{B}(\lambda, \varepsilon)$, *i.e.* $|\lambda - y|_p < \varepsilon$. On rappelle que $\lambda - (y)$ est représenté par la suite $(x_n - y)_{\mathbb{N}}$, et que l'on a défini :

$$|(x_n - y)|_p = \lim_{n \to +\infty} |x_n - y|_p$$

Mais, pour tout $n \geq N$, on a :

$$|x_n - y|_p = |x_n - x_N|_p < \varepsilon'$$

Au passage à la limite quand $n \to +\infty$, on obtient :

$$\lim_{n \to +\infty} |x_n - y|_p \leq \varepsilon' < \varepsilon$$

Donc (y) est bien dans la boule ouvert $\mathcal{B}(\lambda, \varepsilon)$, ce que nous voulions. $\square$

On a alors tous les outils pour montrer que $\mathbb{Q}_p$ est complet pour la valeur absolue p-adique $|\cdot|_p$. Prenons pour cela $(\lambda_n)_{\mathbb{N}}$ une suite de Cauchy de $\mathbb{Q}_p$ (telle que chaque λ_i est la classe d'équivalence d'une suite de Cauchy de $\mathbb{Q}$). Comme $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$, on peut trouver des rationnels $y^{(1)}, y^{(2)}, ..., y^{(n)}, ...$ tels que :

$$\lim_{n \to +\infty} \left|\lambda_n - \left(y^{(n)}\right)\right|_p = 0$$

On montre alors que la suite $\left(y^{(n)}\right)_{\mathbb{N}}$ est une suite de Cauchy et on note λ l'élément de $\mathbb{Q}_p$ lui correspondant. Il ne reste plus qu'à montrer que :

$$\lim_{n \to +\infty} \lambda_n = \lambda$$

Et on a alors bien prouvé que $\mathbb{Q}_p$ est complet.

Maintenant que l'on a construit le corps p-adique $\mathbb{Q}_p$ on peut s'intéresser à la construction de l'anneau des entiers p-adiques à partir de $\mathbb{Q}_p$.

Lemme 2.1.6. Pour tout $x \in \mathbb{Q}_p$, $x \neq 0$, il existe un entier $v_p(x)$ tel que $|x|_p = p^{-v_p(x)}$. En d'autre termes, on peut étendre v_p à $\mathbb{Q}$.

Définition 2.1.8. L'anneau des entiers p-adiques est :

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$$

On peut déjà constater que $\mathbb{Z}_p$ est aussi la boule unité fermée de $\mathbb{Q}_p$ et que c'est un anneau valué.

Définition 2.1.9. Un *anneau local* est un anneau commutatif possédant un unique idéal maximal.

Proposition 2.1.8. L'anneau des entiers p-adiques $\mathbb{Z}_p$ est un anneau local dont l'unique idéal maximal est $p\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p < 1\}$.

Démonstration : Etant donné que $\mathbb{Z}_p$ est un anneau valué, c'est un anneau local. Utilisons le lemme précédent pour montrer que l'idéal est bien engendré par p :

$$|x|_p < 1 \implies |x|_p \leq \frac{1}{p} \implies \left|\frac{x}{p}\right|_p \leq 1 \implies x \in p\mathbb{Z}_p$$

Cela montre que l'idéal valué est inclus dans $p\mathbb{Z}_p$, mais cela suffit puisque l'idéal valué est un idéal maximal et que $p\mathbb{Z}_p \neq \mathbb{Z}_p$. $\square$

Montrons maintenant un résultat important : le lemme de Hensel.

Théorème 2.1.2. *(Lemme de Hensel) Soit $F(X) = a_0 + a_1X + \cdots + a_nX^n$ un polynôme à coefficients dans $\mathbb{Z}_p$. Supposons qu'il existe un entier p-adique $\alpha_1 \in \mathbb{Z}_p$ tel que :*

$$F(\alpha_1) = 0 \pmod{p\mathbb{Z}_p} \quad \textit{et} \quad F'(\alpha_1) \neq 0 \pmod{p\mathbb{Z}_p}$$

où F' est le polynôme dérivé de F. Il existe alors un unique entier p-adique $\alpha \in \mathbb{Z}_p$ tel que :

$$\alpha = \alpha_1 \pmod{p\mathbb{Z}_p} \quad \textit{et} \quad F(\alpha) = 0$$

Démonstration : Commençons par montrer l'existence. Nous allons montrer que la racine α du polynôme existe en construisant une suite d'entiers de Cauchy convergeant vers α.
Soit $(\alpha_n)_{\mathbb{N}}$ une suite de Cauchy telle que, pour tout $n \in \mathbb{N}$:

$$\text{(i) } F(\alpha_n) = 0 \pmod{p^n} \quad \text{et} \quad \text{(ii) } \alpha_n = \alpha_{n+1} \pmod{p^n}$$

Il est facile de voir qu'une telle suite est forcément de Cauchy et que sa limite α vérifiera $F(\alpha) = 0$ (par continuité) et $\alpha = \alpha_1 \pmod{p^n}$ (par construction). Inversement, une racine α va déterminer la suite $(\alpha_n)_{\mathbb{N}}$ voulue. Une fois que l'on aura α_n, le théorème sera donc prouvé.
L'hypothèse du théorème est que α_1 existe. Pour trouver α_2 on utilise la condition (ii) qui implique que :

$$\alpha_2 = \alpha_1 + b_1p$$

avec $b_1 \in \mathbb{Z}_p$. Appliquons cette relation à F et développons, on obtient :

$$\begin{aligned} F(\alpha_2) &= F(\alpha_1 + b_1p) \\ &= F(\alpha_1) + F'(\alpha_1)b_1p + \text{termes en } p^n, \quad n \geq 2 \\ &= F(\alpha_1) + F'(\alpha_1)b_1p \pmod{p^2} \end{aligned}$$

Pour montrer que l'on peut trouver α_2, on doit montrer qu'on peut trouver b_1 tel que :

$$F(\alpha_1) + F'(\alpha_1)b_1p = 0 \pmod{p^2}$$

Maintenant, on sait que $F(\alpha_1) = 0 \pmod p$, donc que $F(\alpha_1) = px$ pour un certain entier x. L'équation précédente devient alors :

$$px + F'(\alpha_1)b_1p = 0 \pmod{p^2}$$

Ce qui nous donne, après avoir divisé par p :

$$x + F'(\alpha_1)b_1 = 0 \pmod p$$

Étant donné que $F'(\alpha_1)$ n'est pas divisible par p, il est inversible dans $\mathbb{Z}_p$, on peut alors prendre :

$$b_1 = -x\left(F'(\alpha_1)\right)^{-1} \pmod p$$

Pour ce choix de b_1, on pose $\alpha_2 = \alpha_1 + b_1p$, qui aura les propriétés voulues.
Par récurrence, on forme α_{n+1} à partir de α_n. On obtient donc la suite recherchée de limite α, ce qui montre l'existence.
Montrons à présent l'unicité. Soit $\alpha' \in \mathbb{Z}_p$ tel que $\alpha' = \alpha \pmod p$ et $F(\alpha') = 0$, alors :

$$0 = F(\alpha') - F(\alpha) = F'(\alpha)(\alpha' - \alpha) + (\alpha' - \alpha)^2 *$$

Si $\alpha' \neq \alpha$, en divisant par $(\alpha' - \alpha)$, on a :

$$0 = F'(\alpha) + (\alpha' - \alpha)*$$

or $F'(\alpha) \in \mathbb{Z}_p^\times$ et $(\alpha' - \alpha) \in p\mathbb{Z}_p$, contradiction. Donc $\alpha = \alpha'$, ce qui montre l'unicité et achève la démonstration. $\square$

2.2 Construction algébrique des corps p-adiques

Dans cette section on donne une construction algébrique de $\mathbb{Q}_p$.

Notation : On note $A_n = \mathbb{Z}/p^n\mathbb{Z}$ l'anneau quotient des entiers modulo p^n. On dispose alors des surjections $\varphi_n : A_{n+1} \to A_n$ de noyau $\ker \varphi_n = p^n A_{n+1}$.

Définition 2.2.1. Un système projectif est la donnée d'une suite $(X_n, \varphi_n)_{n\in\mathbb{N}_{>0}}$ où $(X_n)_{n\in\mathbb{N}_{>0}}$ est une suite d'ensembles et $\varphi_n : X_{n+1} \to X_n$ est une suite d'applications. On la note :

$$\cdots \to X_{n+1} \xrightarrow{\varphi_n} X_n \to \cdots \to X_1$$

On note $X = \varprojlim X_n$ la limite projective, définie par :

$$X = \left\{ x = (x_i)_{i\in\mathbb{N}_{>0}} \in \prod_{i\in\mathbb{N}_{>0}} X_i \mid (\forall i \in \mathbb{N}_{>0})\varphi_i(x_{i+1}) = x_i \right\}$$

De plus si les $(X_n)_{n\in\mathbb{N}_{>0}}$ disposent d'une structure de groupe, d'anneau, ou d'espace topologique (on demande respectivement à ce que les applications $(\varphi_n)_{n\in\mathbb{N}_{>0}}$ soient des morphismes de groupes, d'anneaux, ou continues), alors la limite projective X hérite de la structure correspondante.

Définition 2.2.2. La suite $(\varphi_n)_{n\in\mathbb{N}_{>0}}$ définit un système projectif, on note $\mathbb{Z}_p$ sa limite projective, que l'on appelle *l'anneau des entiers p-adiques*. On montrera que cette définition coïncide avec celle du chapitre précédent.

L'addition et la multiplication se font coordonnées par coordonnées dans $\mathbb{Z}_p$ qui est un sous-anneau de l'anneau produit $A := \prod_n A_n$. On munit A_n de la topologie discrète, et $\prod_n A_n$ de la topologie produit (c'est la topologie la plus fine rendant les projections $\varepsilon_n \colon A \to A_n$ continues, une base d'ouverts étant donnée par les $\bigcap_{i\in I} \varepsilon_i^{-1}(\{x_i\})$ avec $I \subset \mathbb{N}_{>0}$ finie et x_i élément de A_i).

Proposition 2.2.1. On munit $\mathbb{Z}_p \subset A$ de la topologie induite, alors $\mathbb{Z}_p$ est compact.

Démonstration : Pour tout n, A_n est compact donc A est compact (théorème de Tychonov). Si l'on montre que $\mathbb{Z}_p$ est fermé dans A, il est compact car fermé dans un espace compact. □

Lemme 2.2.1. $\mathbb{Z}_p$ est fermé dans A.

Démonstration : On montre que le complémentaire $C := A \setminus \mathbb{Z}_p$ est ouvert. Soit $x \in C$, il existe i tel que $\varphi_i(x_{i+1}) \neq x_i$. Comme A_i est séparé, il existe V_{i+1} et V_i voisinages de $\varphi_i(x_{i+1})$ et x_i respectivement, tels que $V_{i+1} \cap V_i = \emptyset$. Comme φ_i est continue, il existe un voisinage U de x_{i+1} tel que $\varphi_i(U) \subset V_{i+1}$, alors $\varphi_i(U) \cap V_i = \emptyset$ Par conséquent si $y_{i+1} \in U$ et $y_i \in V_i$, on a $\varphi_i(y_{i+1}) \neq y_i$. Donc $\left\{ y = (y_n)_{n>0} \in A \mid y_{i+1} \in U \text{ et } y_i \in V_i \right\}$ est un ouvert contenu dans C .
Autre preuve : $\mathbb{Z}_p$ est le noyau du morphisme de groupes continu $f \colon A \to A$ défini par $f((a_n)_{>0}) = (a_n - \varphi_n(a_{n+1}))_{>0}$. □

On établit quelques propriétés de l'anneau $\mathbb{Z}_p$:

Notation : On note $\varepsilon_n : \mathbb{Z}_p \to A_n$ la projection sur la n-ième composante (c'est un morphisme d'anneaux), et $p^n : \mathbb{Z}_p \to \mathbb{Z}_p$ la multiplication par p^n.

Proposition 2.2.2. La suite $0 \to \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} A_n \to 0$ est exacte.

Démonstration : (i) On montre que $\ker(p^n) = \{0\}$. Il suffit de vérifier que la multiplication par p est injective. Soit $x = (x_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p$. Si $px = 0$ alors $px_{n+1} = 0$ pour tout $n \in \mathbb{N}$ (égalité dans A_{n+1}). Pour tout $n \in \mathbb{N}$, il existe donc $k_n \in A_{n+1}$ tel que $x_{n+1} = p^n k_n$, et pour tout $n \in \mathbb{N}$, $x_n = \varphi_n(x_{n+1}) = p^n \varphi_n(k_n) \pmod{p^n} = 0$, donc $x = 0$.

(ii) $\ker(\varepsilon_n) = \mathrm{Im}(p^n) = p^n\mathbb{Z}_p$: l'inclusion $p^n\mathbb{Z}_p \subset \ker(\varepsilon_n)$ est immédiate. Réciproquement, si $x \in \ker(\varepsilon_n)$, on a $x_n = 0$, donc $\varphi_n(x_{n+1}) = x_n = 0 \pmod{p^n}$, et de proche en proche $x_m = 0 \pmod{p^n}$ pour tout $m \geq n$. On écrit alors $x_m = p^n y_{m-n}$, où $y_{m-n} \in A_{m-n}$, et on pose $y = (y_i)_{i\geq 0}$. On a bien $y \in \mathbb{Z}_p$ puisque $y_i \in A_i$ et $\varphi_i(y_{i+1}) = y_i$ pour tout i. (En effet $\varphi_m(x_{m+1}) = x_m = p^n y_{m-n} \pmod{p^m}$ d'une part et $\varphi_m(x_{m+1}) = x_{m+1} \pmod{p^m} = p^n y_{m+1-n} \pmod{p^m}$ d'autre part, ce qui donne l'égalité $p^n y_{m-n} \pmod{p^m} = p^n y_{m+1-n} \pmod{p^m}$. D'où $y_{m-n} = y_{m+1-n} \pmod{p^{m-n}}$ pour tout $m \geq n$). On a alors $x = p^n y \in p^n\mathbb{Z}_p$, d'où l'inclusion réciproque. □

Corollaire 2.2.1. On a l'isomorphisme d'anneaux $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Démonstration : On factorise le morphisme d'anneaux ε_n ci-dessus. □

Proposition 2.2.3. i) Notons $\mathbb{U}$ le groupe des inversibles de $\mathbb{Z}_p$, dont un élément est appelé *unité p-adique*. On a $\mathbb{U} = \{x \in \mathbb{Z}_p \mid p \nmid x\}$.
ii) Tout élément de $\mathbb{Z}_p \setminus \{0\}$ s'écrit de façon unique $p^n u$ avec $n \in \mathbb{N}$ et $u \in \mathbb{U}$.

Démonstration : (i) On a déjà le résultat pour les A_n, puisque $(\mathbb{Z}/p^n\mathbb{Z})^\times = (\mathbb{Z}/p^n\mathbb{Z}) \setminus p(\mathbb{Z}/p^n\mathbb{Z})$. Ensuite, si $x \in \mathbb{Z}_p$ tel que $p \nmid x$, alors $p \nmid x_n$ pour tout n et x_n est inversible, donc x l'est aussi puisque $A^\times = \prod_{n>0} A_n^\times$. Vérifions que son inverse appartient à $\mathbb{Z}_p$. Soit $y \in A$ tel que $xy = 1$, alors $x_n y_n = 1$ pour tout $n > 0$. Cela donne $x_{n-1}\varphi_{n-1}(y_n) = 1$, et par unicité de l'inverse de x_{n-1} dans A_{n-1}, on a $y_{n-1} = \varphi_{n-1}(y_n)$.
(ii) Soit $x \in \mathbb{Z}_p \setminus \{0\}$ et n le plus grand entier tel que $x_n = \varepsilon_n(x)$ soit nul. On a alors $x = p^n u$ $(x = (0, \ldots, 0, p^k u_{k+1}, p^k u_{k+2}, \ldots))$ avec $p \nmid u$, donc $u \in \mathbb{U}$ par (i).
Enfin si $p^n u = p^m v$ alors $p^{n-m} = vu^{-1} \in \mathbb{U}$ n'est pas divisible par p, donc $n = m$ et $u = v$.□

Notation : On note $v_p(x)$ l'entier n dans l'écriture précédente, appelé la *valuation p-adique* de x. Si $x = 0$ on pose par convention $v_p(0) = +\infty$.
On vérifie que $v_p(xy) = v_p(x) + v_p(y)$ et $v_p(x+y) \geq \inf(v_p(x), v_p(y))$, et que $\mathbb{Z}_p$ est un anneau intègre et principal. (Si $x, y \in \mathbb{Z}_p$ sont non nuls alors $v_p(xy) = v_p(x) + v_p(y) < +\infty$, et les idéaux sont de la forme $p^n\mathbb{Z}_p$ où $n = \min\{v_p(x) \mid x \in I\}$).

Proposition 2.2.4. Soit $\mathrm{d}(x, y) = e^{-v_p(x-y)}$. C'est une distance sur $\mathbb{Z}_p$ dont la topologie associée coïncide avec la topologie sur $\mathbb{Z}_p$ définie précédemment.
$\mathbb{Z}_p$ est un espace complet, et $\mathbb{Z}$ est dense dans $\mathbb{Z}_p$.

Démonstration : d est une distance sur $\mathbb{Z}_p$ car pour tous $x, y, z \in \mathbb{Z}_p$:
• $\mathrm{d}(x, y) = \mathrm{d}(y, x)$ et $\mathrm{d}(x, x) = e^{-v_p(0)} = e^{-\infty} = 0$

• si $\mathrm{d}(x, y) = 0$ alors $e^{-v_p(x-y)} = 0$ donc $v_p(x - y) = +\infty$ et $x = y$.

• $\mathrm{d}(x, y) = e^{-v_p(x-y)} = e^{-v_p((x-z)+(z-y))} \leq e^{-\min(v_p(x-z), v_p(z-y))}$
$\leq \max(e^{-v_p(x-z)}, e^{-v_p(z-y)}) = \max(\mathrm{d}(x, z), \mathrm{d}(z, y))$
On dit que d est une distance *ultramétrique*.

Pour montrer que les topologies considérées coïncident, on va déterminer une base d'ouverts de $\mathbb{Z}_p$ pour chacune :

D'une part, une prébase de A est donnée par les parties de la forme :

$$A_1 \times \cdots \times A_{i-1} \times \{x_i\} \times A_{i+1} \times \cdots \text{ où } i \in \mathbb{N}_{n>0} \text{ et } x_i \in A_i$$

donc une base $B =$ est donnée par les parties de la forme :

$$\prod_{n=1}^{i} \{x_n\} \times \prod_{n>i} A_n \text{ pour } i \in \mathbb{N}_{>0} \text{ et } x_n \in A_n \text{ pour tout } n \in \{1, \ldots, i\}$$

et une base de $\mathbb{Z}_p$ est donc donnée par les éléments de $B \cap \mathbb{Z}_p$.
D'autre part les boules ouvertes pour d sont données par : si $a = (a_n) \in \mathbb{Z}_p$ et $\varepsilon > 0$, on a :

$$x \in B(a, \varepsilon) \Leftrightarrow v_p(x-a) > -\ln\varepsilon \Leftrightarrow v_p(x-a) > \lfloor -\ln\varepsilon \rfloor =: n_0$$

Donc $B(a, \varepsilon) = \Big(\{a_1\} \times ... \times \{a_{n_0}\} \times \prod_{i \geq n_0+1} A_i\Big) \cap \mathbb{Z}_p$, et les topologies coïncident.
Pour la densité de $\mathbb{Z}$ dans $\mathbb{Z}_p$, on montre que tout ouvert de $\mathbb{Z}_p$ intersecte $\mathbb{Z}$: si

$$U = \Big(\{x_1\} \times ... \times \{x_n\} \times \prod_{i \geq n+1} A_i\Big) \cap \mathbb{Z}_p$$

est un ouvert de la base, alors $x_n \in \mathbb{Z}$ s'écrit $(x_1, ..., x_n, x_n, ...) \in U$.
Enfin $\mathbb{Z}_p$ est complet car c'est un espace métrique compact. □

Définition 2.2.3. Le corps des nombres p-adiques, noté $\mathbb{Q}_p$ est défini comme étant le corps des fractions des entiers p-adiques : $\mathbb{Q}_p :=$Frac$(\mathbb{Z}_p)$.

Les éléments $x \in \mathbb{Q}_p^\times$ s'écrivent de façon unique $x = p^n u$ avec $n \in \mathbb{Z}$ et $u \in \mathbb{U}$, de sorte que $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$. On pose $v_p(x) = n$, ce qui étend la valuation p-adique à $\mathbb{Q}_p$. Remarquons que $v_p(x) \geq 0 \Leftrightarrow x \in \mathbb{Z}_p$.

Proposition 2.2.5. On prolonge la distance d à $\mathbb{Q}_p$, alors :
(i) $\mathbb{Z}_p$ est un sous-anneau ouvert et fermé ;
(ii) $\mathbb{Q}_p$ est localement compact ;
(iii) $\mathbb{Q}_p$ est complet.

Démonstration : (i) On vérifie que $\mathbb{Z}_p = B'(0,1) = \{x \in \mathbb{Q}_p \mid v_p(x) \geq 0\} = B(0, e)$.
(ii) Il s'agit de montrer que tout point admet un voisinage compact. D'après le premier point, pour tout $x \in \mathbb{Q}_p$, $x + \mathbb{Z}_p$ est un voisinage de x, qui est compact car $\mathbb{Z}_p$ est compact.
(iii) $\mathbb{Q}_p$ est complet car c'est un groupe topologique localement compact. [*c.f.* Appendice] □

Proposition 2.2.6. Les deux constructions de $\mathbb{Q}_p$ sont isomorphes. Plus précisément, il existe une isométrie bijective $\varphi : \mathbb{Q}_{p,analytique} \to \mathbb{Q}_{p,alg.}$, telle que, si i est l'injection : $\mathbb{Q} \hookrightarrow \mathbb{Q}_{p,alg.}$, on ait $\varphi \circ \mathrm{Id}_{\mathbb{Q}} = i$.)

Démonstration : Les distances d et $|\cdot|_p$ sont équivalentes, et la proposition résulte de la propriété universelle du complété. □

Par conséquent les résultats énoncés dans la partie précédente restent valables.

2.3 Opérations sur les corps p-adiques

2.3.1 Equations p-adique

Lemme 2.3.1. Soit $\cdots \to X_n \to X_{n-1} \to \cdots \to X_1$ un système projectif d'ensembles et $X = \varprojlim X_n$. Si les X_n sont finis et non vides, alors X est non vide.

Démonstration : On se ramène au cas où les applications $X_n \to X_{n-1}$ sont surjectives. Fixons n, et notons $X_{n,p}$ l'image de X_{n+p} dans X_n. La suite $(X_{n,p})_{p\geq 0}$ est une suite décroissante. (En effet si $x \in X_{n,p+1}$ alors il existe $y \in X_{n+p+1}$ tel que $x = \varphi_n \circ \cdots \circ \varphi_{n+p}(y)$, avec $\varphi_{n+p}(y) \in X_{n+p}$). C'est donc une suite stationnaire, notons Y_n l'ensemble "limite". Comme $\varphi_n(X_{n+1,p}) = X_{n,p+1}$, on obtient $\varphi_n(Y_{n+1}) = Y_n$ en prenant p assez grand. Enfin les Y_n sont non vides, donc $\varprojlim Y_n \neq \emptyset$ et $\varprojlim X_n \neq \emptyset$. □

Remarque : Prenons $X_n = \mathbb{N}$ pour tout $n > 0$, et soit $\varphi_n(x) = x+1$. La suite $(X_n, \varphi_n)_{n\in\mathbb{N}_{>0}}$ définit un système projectif, mais $X = \varprojlim X_n = \emptyset$. En effet, si $(x_n)_{n>0} \in X$, on a $\varphi_n(x_{n+1}) = x_n - 1 \neq x_n$, ce qui est absurde.

Notation : Pour $f \in \mathbb{Z}_p[X_1, ..., X_m]$, on note $f_n \in A_n[X_1, ..., X_m]$ le polynôme dont les coefficients sont les n-ièmes composantes de ceux de f.

Proposition 2.3.1. Soit $(f^{(i)})_{i\in I}$ une famille d'éléments de $\mathbb{Z}_p[X_1, \ldots, X_m]$. On a l'équivalence :

(i) Les $f^{(i)}$ ont un zéro commun dans $(\mathbb{Z}_p)^m$;
(ii) Pour tout $n \geq 1$, les $f_n^{(i)}$ ont une zéro commun dans $(A_n)^m$.

Démonstration : Soit X (respectivement X_n) l'ensemble des zéros communs des $f^{(i)}$ (resp. des $f_n^{(i)}$). On a alors $X = \varprojlim X_n$ de sorte que X est non vide si et seulement si les X_n sont non vides. □

Définition 2.3.1. On dit que $x = (x_1, \ldots, x_m) \in \mathbb{Z}_p^m$(resp. $\in A_n^m$) est *primitif* si l'un des x_i est inversibles (i.e. si l'un des x_i n'est pas divisible par p).

Proposition 2.3.2. Soit $(f^{(i)})_{i\in I}$ une famille de polynômes homogènes dans $\mathbb{Z}_p[X_1, \ldots, X_m]$. On a les équivalences :

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

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

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

Démonstration : On a déjà (ii) $\Rightarrow$ (i) et (ii) $\Leftrightarrow$ (iii) d'après la proposition précédente. Montrons (i) $\Rightarrow$ (ii) : soit $x = (x_1, \ldots, x_m)$ un zéro commun non trivial des $f^{(i)}$, et $n = \min(v_p(x_1), \ldots, v_p(x_m))$. Posons $y = p^{-n}x$. C'est un élément primitif de $(\mathbb{Z}_p)^m$ qui est un zéro commun des $f^{(i)}$ par homogénéité. $\square$

2.3.2 Lemme de Hensel

On montre dans cette section une version généralisée et algébrique du lemme de Hensel (ou méthode de Newton).

Lemme 2.3.2. Soient $f \in \mathbb{Z}_p[X]$, $x \in \mathbb{Z}_p$, $n, k \in \mathbb{Z}$ tels que :

$$0 < 2k < n,\ f(x) = 0 \pmod{p^n} \text{ et } v_p(f'(x)) = k.$$

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

$$f(y) = 0 \pmod{p^{n+1}},\ v_p(f'(y)) = k \text{ et } y = x \pmod{p^{n-k}}.$$

Démonstration : On cherche y de la forme $x + p^{n-k}z$ avec $z \in \mathbb{Z}_p$. La formule de Taylor appliquée à f en y s'écrit :

$$f(y) = f(x) + p^{n-k}zf'(x) + p^{2n-2k}a$$

avec $a \in \mathbb{Z}_p$. Comme $f(x) = p^n b$ et $f'(x) = p^k u$ avec $b \in \mathbb{Z}_p$ et $u \in \mathbb{U}$ par hypothèse, on prend $z = bu^-1$ qui vérifie $b + zu = 0$. On obtient $f(y) = p^{2n-2k}a = 0 \mod p^{n+1}$ puisque $2n - 2k > n$. La formule de Taylor appliquée à f' en y s'écrit $f'(y) = f'(x) + p^{n-k}d$ où $d \in \mathbb{Z}_p$, ce qui donne $f'(y) = p^k u \pmod{p^{n-k}}$ (car $n - k > k$), d'où $v_p(f'(y)) = k$. $\square$

Théorème 2.3.1. *Soient $f \in \mathbb{Z}_p[X_1, \ldots, X_m]$, $x = (x_i) \in \mathbb{Z}_p^m$, $n, k, j \in \mathbb{Z}$ tels que $1 \leq j \leq m$, $0 \leq 2k < n$, on suppose que $f(x) = 0 \pmod{p^n}$ et $v_p(\frac{\partial f}{\partial X_j}(x)) = k$. Alors il existe un zéro $y \in \mathbb{Z}_p^m$ de f tel que $y = x \mod p^{n-k}$.*

Démonstration : Pour $m = 1$, on applique le lemme avec $x^{(0)} := x$, ce qui fournit $x^{(1)} \in \mathbb{Z}_p$ tel que $x^{(1)} = x^{(0)} \mod p^{n-k}$ tel que $f(x^{(1)}) = 0 \mod p^{n+1}$ et $v_p(f'(x^{(1)})) = k$. On applique de nouveau le lemme à $x^{(1)}$ (en remplaçant n par $n+1$), ce qui fournit de proche en proche une suite $x^{(0)}, \ldots, x^{(q)}, \ldots,$ telle que : $x^{(q+1)} = x^{(q)} \mod p^{n+q-k}$ et $f(x^{(q)}) = 0 \mod p^{n+q}$. C'est une suite de Cauchy ; notons y sa limite. Elle vérifie $f(y) = 0$ et $y = x \mod p^{n-k}$.

Pour $m > 1$, on se ramène au cas où $m = 1$. Notons $\widetilde{f} \in \mathbb{Z}_p[X_j]$ le polynôme $f(x_1, \ldots, X_j, \ldots, x_m)$. On applique le cas précédent à $\widetilde{f}$ et x_j, alors il existe $y_j = x_j \mod p^{n-k}$ tel que $\widetilde{f}(y_j) = 0$, et $y = (x_1, \ldots, y_j, \ldots, x_m)$ convient. $\square$

Corollaire 2.3.1. Tout zéro simple de f modulo p se relève en un zéro dans $\mathbb{Z}_p$. Plus précisément si $f(x) = 0 \mod p$ et s'il existe j tel que $v_p(\frac{\partial f}{\partial X_j}(x)) \neq 0$ alors il existe $y \in \mathbb{Z}_p$ tel que $f(y) = 0$ et $y = x \mod p$.
(Un zéro x de f est dit simple si l'une des dérivées partielles $\frac{\partial f}{\partial X_j}(x)$ est non nulle.)

Démonstration : C'est un cas particulier du théorème pour $n = 1$ et $k = 0$. □

Corollaire 2.3.2. Si $p \neq 2$, soit $f(X) = \sum_{1 \leq i,j \leq n} a_{i,j} X_i X_j$ avec $a_{i,j} = a_{j,i}$ une forme quadratique à coefficients dans $\mathbb{Z}_p$ telle que $\det(a_{i,j}) \in \mathbb{U}$. Soit $a \in \mathbb{Z}_p$. Alors toute solution primitive de l'équation $f(x) = a \mod p$ se relève en une solution exacte dans $\mathbb{Z}_p$.

Démonstration : D'après le corollaire précédent, il suffit de vérifier que l'une des dérivées partielles n'est pas nulle. On a $\frac{\partial f}{\partial X_j} = 2 \sum_{1 \leq i \leq n} a_{i,j} X_i$. Notons $X = (x_i)_i$ et $M = (a_{i,j})_{i,j}$. Si toutes les dérivées étaient nulles, on aurait $XM = 0$, donc $X = 0$ puisque $\det M \in \mathbb{U}$ est inversible. □

Corollaire 2.3.3. Si $p = 2$, soit f une forme quadratique comme ci-dessus, à coefficients dans $\mathbb{Z}_2$, et $a \in \mathbb{Z}_2$. Si x est une solution primitive de $f(x) = a \mod 8$, alors on peut relever x en une solution exacte s'il existe j tel que $\frac{\partial f}{\partial X_j}(x) \neq 0 \mod 4$. (Cette condition est en particulier vérifiée lorsque $\det(a_{i,j}) \in \mathbb{U}$).

Démonstration : Cela résulte du théorème avec $n = 3$ et $k = 1$. □

2.4 Le groupe multiplicatif de $\mathbb{Q}_p$

Soit $n \geq 1$ et $\mathbb{U}_n := 1 + p^n\mathbb{Z}_p = \ker \pi_n$ où $\pi_n \colon \mathbb{U} \to (\mathbb{Z}/p^n\mathbb{Z})^*$ est la surjection canonique. On a en particulier $\mathbb{U}/\mathbb{U}_1 \simeq \mathbb{F}_p^*$, qui est cyclique d'ordre $p-1$. Les $\mathbb{U}_n$ forment une suite décroissante de sous groupes ouverts de $\mathbb{U}$ et $\mathbb{U} \simeq \varprojlim \mathbb{U}/\mathbb{U}_n$. En effet cela résulte du lemme suivant :

Lemme 2.4.1. Soit $G = \varprojlim G_n$ une limite projective de groupes, et soient $\psi_n : G \to G_n$. Alors $G' := \bigcap \ker \psi_n = \{e\}$ et $G \simeq \varprojlim (G/\ker \psi_n)$.

Ensuite, si $1+p^n x$ et $1+p^n y$ sont des éléments de $\mathbb{U}_n$, on a : $(1+p^n x)(1+p^n y) = 1+p^n(x+y) \mod p^{n+1}$. Soit alors le morphisme $\varphi : \mathbb{U}_n \to \mathbb{Z}/p\mathbb{Z}$ défini par $\varphi(1+p^n x) = x \mod p$. On a $\varphi((1+p^n x)(1+p^n y)) = x+y \mod p$ et $\ker \varphi = \mathbb{U}_{n+1}$ d'où l'isomorphisme $\mathbb{U}_n/\mathbb{U}_{n+1} \simeq \mathbb{Z}/p\mathbb{Z}$. D'après la formule de l'indice, on a alors $\mathrm{Card}(\mathbb{U}_1/\mathbb{U}_n) = p^{n-1}$.

Lemme 2.4.2. Soit $0 \to A \to E \to B \to 0$ une suite exacte de groupes commutatifs, avec A et B finis d'ordres premiers entre eux a et b respectivement. Soit $B' := \{x \in E, bx = 0\}$. Alors on a la somme directe $E = A \bigoplus B'$ et B' est le seul sous-groupe de E isomorphe à B.

Démonstration : Soient $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Si $x \in A \cap B'$ alors $ax = bx = 0$, donc $(au + bv)x = x = 0$, ce qui montre que $A \cap B' = \{0\}$. Si $x \in E$, alors x s'écrit $x = aux + bvx$, où $aux \in B'$ et $bvx \in A$. En effet, $bB = 0$ donc $bE \subset A$ (car A est le noyau de $E \to B$), donc $bvx \in A$. De plus $abE = 0$, d'où $aux \in B'$.
D'autre part, la projection $E = A \bigoplus B' \to B$ définit un isomorphisme entre B' et B. Si B'' est un autre sous-groupe de E isomorphe à B alors $bB'' = 0$, donc $B'' \subset B'$ et $B' = B''$ puisqu'ils sont de même ordre. □

Proposition 2.4.1. On a $\mathbb{U} = \mathbb{V} \times \mathbb{U}_1$ où $\mathbb{V} := \{x \in \mathbb{U} \mid x^{p-1} = 1\}$ est le seul sous-groupe de $\mathbb{U}$ isomorphe à $\mathbb{F}_p^\times$.

Démonstration : Cela résulte du lemme appliqué aux suites exactes $1 \to \mathbb{U}_1/\mathbb{U}_n \to \mathbb{U}/\mathbb{U}_n \to \mathbb{F}_p^\times \to 1$, l'ordre de $\mathbb{U}_1/\mathbb{U}_n$ étant p^{n-1} qui est premier avec $p-1$ l'ordre de $\mathbb{F}_p^\times$. On en déduit qu'il existe un unique sous-groupe $\mathbb{V}_n$ de $\mathbb{U}/\mathbb{U}_n$ isomorphe à $\mathbb{F}_p^\times$, et que la projection $\mathbb{U}/\mathbb{U}_n \to \mathbb{U}/\mathbb{U}_{n-1}$ induit un isomorphisme $\mathbb{V}_n \simeq \mathbb{V}_{n-1}$. Comme $\mathbb{U} = \varprojlim \mathbb{U}/\mathbb{U}_n$, on en déduit par passage à la limite un sous-groupe $\mathbb{V}$ de $\mathbb{U}$ isomorphe à $\mathbb{F}_p^\times$. □

Le groupe $\mathbb{V}$ s'appelle le groupe des représentants multiplicatifs des éléments de $\mathbb{F}_p^\times$.

Corollaire 2.4.1. Le corps $\mathbb{Q}_p$ contient les racines $(p-1)$-ièmes de l'unité.

On étudie désormais la structure du groupe $\mathbb{U}_1$.

Lemme 2.4.3. Soit $x \in \mathbb{U}_n \setminus \mathbb{U}_{n+1}$ et $n \geq 1$ si $p \neq 2$ et $n \geq 2$ si $p = 2$. Alors $x^p \in \mathbb{U}_{n+1} \setminus \mathbb{U}_{n+2}$.

Démonstration : Par hypothèse $x = 1 + kp^n$ avec $p \nmid k$. D'après la formule du binôme, on a : $x^p = 1 + kp^{n+1} \cdots + k^p p^{np}$, ce qui se réduit modulo p^{n+2} en $x^p = 1 + kp^{n+1} \mod p^{n+2}$. □

Proposition 2.4.2. Si $p \neq 2$, alors $\mathbb{U}_1 \simeq \mathbb{Z}_p$. Si $p = 2$ alors $\mathbb{U}_1 = \{\pm 1\} \times \mathbb{U}_2$ et $\mathbb{U}_2 \simeq \mathbb{Z}_2$.

Démonstration : Pour $p \neq 2$: Soit $x \in \mathbb{U}_1 \setminus \mathbb{U}_2$ (par exemple $x = 1 + p$ convient). D'après le lemme, on a $x^{p^i} \in \mathbb{U}_{i+1} \setminus \mathbb{U}_{i+2}$. Soit x_n l'image de x dans $\mathbb{U}_1/\mathbb{U}_n$. On a donc : $x_n^{p^{n-2}} \neq 1$ et $x_n^{p^{n-1}} = 1$. Comme $\mathbb{U}_1/\mathbb{U}_n$ est d'ordre p^{n-1} on en déduit qu'il est cyclique et que x_n est un générateur. Notons $\theta_{n,x}$ l'isomorphisme $k \mapsto x_n^k$ de $\mathbb{Z}/p^{n-1}\mathbb{Z}$ sur $\mathbb{U}_1/\mathbb{U}_n$. Le diagramme suivant est commutatif :

$$\begin{array}{ccc}
\mathbb{Z}/p^n\mathbb{Z} & \xrightarrow{\theta_{n+1,x}} & \mathbb{U}_1/\mathbb{U}_{n+1} \\
\downarrow & & \downarrow \\
\mathbb{Z}/p^{n-1}\mathbb{Z} & \xrightarrow{\theta_{n,x}} & \mathbb{U}_1/\mathbb{U}_n
\end{array}$$

Lemme 2.4.4. Soient $(X_n, \varphi_n)_{n\in\mathbb{N}>0}$, $(Y_n, \psi_n)_{n\in\mathbb{N}>0}$ deux systèmes projectives de limites projectives respectives X et Y. Supposons que pour tout $n > 0$, il existe un isomorphisme $f_n \colon X_n \xrightarrow{\sim} Y_n$ vérifiant la relation de compatibilité suivante : $\psi_n \circ f_{n+1} = f_n \circ \varphi_n$. Notons $\varepsilon_n : X \to X_n$ et $\mu_n : Y \to Y_n$ les surjections canoniques, alors il existe un isomorphisme $f : X \to Y$ vérifiant $\mu_n \circ f = f_n \circ \varepsilon_n$ pour tout $n > 0$.

On déduit un isomorphisme de $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^{n-1}\mathbb{Z}$ sur $\mathbb{U}_1 = \varprojlim \mathbb{U}_1/\mathbb{U}_n$, i.e. $(\mathbb{U}_1, \cdot) \simeq (\mathbb{Z}_p, +)$.

Démonstration du lemme : Soit $f : X \to Y$ définie par $f(x) = (f_n \circ \varepsilon_n(x))_{n\in\mathbb{N}}$. Elle est bien définie car $\psi_n \circ f_n \circ \varepsilon_n = f_{n-1} \circ \varepsilon_{n-1}$. Elle est surjective car si $y = (y_n)_{n\in\mathbb{N}} \in Y$, alors il existe $x_n \in X_n$ unique tel que $y_n = f_n(x_n)$, et $x = (x_n)_{n>0} \in X$ puisque $\psi_n(y_n) = y_{n-1} \Rightarrow \psi_n \circ f_n(x_n) = f_{n-1} \circ \varphi_n(x_n) = f_{n-1}(x_{n-1}) \Rightarrow \varphi_n(x_n) = x_{n-1}$. Elle est injective par injectivité de f_n, et par le fait que $x = (\varepsilon_n(x))_{n\in\mathbb{N}}$. $\square$

Pour $p = 2$: soit $x \in \mathbb{U}_2 \setminus \mathbb{U}_3$. En écrivant $x = 1 + 4k$ avec $k = 2m + 1$ impair, on obtient que $x = 5 + 8m$ d'où $x = 5 \mod 8$. On peut encore définir les isomorphismes $\theta_{n,x} : \mathbb{Z}/2^{n-2}\mathbb{Z} \to \mathbb{U}_2/\mathbb{U}_n$ qui définissent un isomorphisme $\mathbb{Z}_2 \to \mathbb{U}_2$. Comme $\mathbb{U}_1/\mathbb{U}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ on a bien $\mathbb{U}_1 \simeq \{\pm 1\} \times \mathbb{U}_2$. $\square$

Théorème 2.4.1. *On a l'isomorphisme :*

$$\mathbb{Q}_p^\times \simeq \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$$

si $p \neq 2$ et

$$\mathbb{Q}_2^\times \simeq \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}.$$

Démonstration : Soit $x \in \mathbb{Q}_p^\times$, on écrit $x = p^n u$ où $u \in \mathbb{U}$ et $n \in \mathbb{Z}$, ce qui montre que $\mathbb{Q}_p^* \simeq \mathbb{Z} \times \mathbb{U}$. On a déterminé précédemment la structure du groupe $\mathbb{U} = \mathbb{V} \times \mathbb{U}_1$ où $\mathbb{V}$ est cyclique d'ordre $p - 1$. Enfin, la structure de $\mathbb{U}_1$ est donnée par la proposition ci-dessus. $\square$

Déterminons à présent les carrés de $\mathbb{Q}_p^\times$.

Théorème 2.4.2. *Si $p \neq 2$, soit $x = p^n u \in \mathbb{Q}_p^\times$ (où $n \in \mathbb{Z}$, $u \in \mathbb{U}$). On a l'équivalence : x est un carré si et seulement si n est pair et l'image $\tilde{u}$ de u dans $\mathbb{U}/\mathbb{U}_1 \simeq \mathbb{F}_p^\times$ est un carré.*

Démonstration : Écrivons $u = v \cdot u_1$ où $v \in \mathbb{V}$ et $u_1 \in \mathbb{U}_1$. D'après le théorème précédent, $\mathbb{Q}_p^\times \simeq \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ et x est un carré si et seulement si n est pair et v et u_1 sont des carrés. Comme $(\mathbb{U}_1, \cdot) \simeq (\mathbb{Z}_p, +)$, et que $2 \in \mathbb{U}$, tout élément de $\mathbb{U}_1$ est un carré. Enfin, on a l'isomorphisme $\mathbb{V} \simeq \mathbb{F}_p^\times$. $\square$

Remarque : La deuxième condition s'exprime par $(\frac{\tilde{u}}{p}) = 1$ ce qui sera noté simplement $(\frac{u}{p})$.

Corollaire 2.4.2. Si $p \neq 2$, le groupe $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ est un groupe de type $(2, 2)$ qui admet pour représentants $\{1, p, u, up\}$ où $u \in \mathbb{U}$ est tel que $(\frac{u}{p}) = -1$.

Démonstration : On quotiente $\mathbb{Q}_p^\times \simeq \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{F}_p^\times$ par $\mathbb{Q}_p^{\times 2} \simeq 2\mathbb{Z} \times \mathbb{Z}_p \times \mathbb{F}_p^{\times 2}$, où $\mathbb{F}_p^{\times 2}$ est le sous-groupe d'indice 2 dans $\mathbb{F}_p^\times$, donc $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Les représentants non triviaux sont donnés par les classes non triviales du quotient. □

Théorème 2.4.3. *Si $p = 2$, soit $x = 2^n u \in \mathbb{Q}_2^\times$. On a l'équivalence : x est un carré si et seulement si n est pair et $u = 1 \mod 8$.*

Démonstration : On a $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \simeq (2^{\mathbb{Z}}/2^{2\mathbb{Z}}) \times (\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2)$. Comme $\mathbb{Z}_2^\times = 1 + 2\mathbb{Z}_2 = \{\pm 1\} \times \mathbb{U}_2 = \{\pm 1\} \cdot (1 + 4\mathbb{Z}_2)$, on a $\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 \simeq \{\pm 1\} \cdot (1 + 4\mathbb{Z}_2)/(1 + 8\mathbb{Z}_2)$ si l'on montre que $(\mathbb{Z}_2^\times)^2 = \mathbb{U}_3 = 1 + 8\mathbb{Z}_2$.

Lemme 2.4.5. $u \in \mathbb{Z}_2^\times$ est un carré si et seulement si $u \in 1 + 8\mathbb{Z}_2$

Démonstration du lemme : Si $u = v^2 \in (\mathbb{Z}_2^\times)^2$. Écrivons $v = 1 + 2k$ où $k \in \mathbb{Z}_2$, on a alors : $v^2 = 1 + 4k(1 + k)$, avec $2 \mid k$ ou $2 \mid 1 + k$ d'où $u = v^2 \in 1 + 8\mathbb{Z}_2$. Réciproquement, si $u \in 1 + 8\mathbb{Z}_2$, soit $f(X) = X^2 - u$. On applique le lemme de Hensel à la solution approchée : 1 mod 8, avec les paramètres $p = 2$, $n = 3$ et $k = 1$. Cela fournit un zéro $y \in \mathbb{Z}_p$ tel que $y = u \pmod 4$.
Ainsi $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \simeq \mathbb{Z}/2\mathbb{Z} \times \{\pm 1\} \cdot (1 + 4\mathbb{Z}_2)/(1 + 8\mathbb{Z}_2)$. □

Corollaire 2.4.3. Le groupe $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ est de type $(2, 2, 2)$. Il admet pour représentants $\{\pm 1, \pm 5, \pm 2, \pm 10\}$.

Démonstration : On quotiente $\mathbb{Q}_2^\times \simeq \mathbb{Z} \times \mathbb{U}$ par $\mathbb{Q}_2^{\times 2} \simeq 2\mathbb{Z} \times \mathbb{U}_3$. Comme $\mathbb{U}/\mathbb{U}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{U}_2/\mathbb{U}_3 \simeq \mathbb{Z}/2\mathbb{Z}$, on a : $\mathbb{U}/\mathbb{U}_3$ est groupe d'ordre 4, isomorphe à $(1 + 4\mathbb{Z}_2)/(1 + 8\mathbb{Z}_2)$ donc ses éléments sont d'ordre divisant 4, et $\mathbb{U}/\mathbb{U}_3 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. De plus l'isomorphisme $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \simeq \mathbb{Z}/2\mathbb{Z} \times \{\pm 1\} \cdot (1 + 4\mathbb{Z}_2)/(1 + 8\mathbb{Z}_2)$ fournit les représentants. □

Remarque : Soient $\varepsilon, \omega : \mathbb{U}/\mathbb{U}_2 \to \mathbb{Z}/2\mathbb{Z}$ définis par $\varepsilon(z) = \frac{z-1}{2} \mod 2$ et $\omega(z) = \frac{z^2-1}{8} \mod 2$, ce sont respectivement des isomorphismes de $\mathbb{U}/\mathbb{U}_2$ sur $\mathbb{Z}/2\mathbb{Z}$ et de $\mathbb{U}_2/\mathbb{U}_3$ sur $\mathbb{Z}/2\mathbb{Z}$.

Corollaire 2.4.4. Si $p \neq 2$, les extensions quadratiques de $\mathbb{Q}_p$ sont les

$$\mathbb{Q}_p[\sqrt{d}]$$

où $d \in \{p, u, up\}$ avec $u \in \mathbb{U}$ et $\left(\dfrac{u}{p}\right) = -1$.
Si $p = 2$ il y a exactement 7 extensions quadratiques de $\mathbb{Q}_2$:

$$\mathbb{Q}_2[\sqrt{-1}]\ \mathbb{Q}_2[\sqrt{\pm 5}]\ \mathbb{Q}_2[\sqrt{\pm 2}]\ \mathbb{Q}_2[\sqrt{\pm 10}].$$

Démonstration : On sait que les extensions quadratiques d'un corps de caractéristique nulle ($\mathbb{Q}_p$ contient un sous-corps isomorphe à $\mathbb{Q}$) sont de la forme $\mathbb{Q}[\sqrt{d}]$, où d est sans facteur carré. Les représentants des classes non triviales de $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ fournissent les extensions quadratiques.

Corollaire 2.4.5. Les carrés forment un sous-groupe ouvert de $\mathbb{Q}_p^*$.

Démonstration : Soit $x \in \mathbb{Q}_p^{*2}$ un carré. On a $x \in B_{|\cdot|_p}(x, |x|_p) \subset \mathbb{Q}_p^{*2}$. En effet, soit $y \in B_{|\cdot|_p}(x, |x|_p)$, alors $v_p(x-y) > v_p(x) = 2n$ pour un certain entier n, donc $x = y + p^k v$ où $k > 2n$ et $v \in \mathbb{U}$. D'où $y = p^{2n}(u - p^{k-2n}v)$ et $\left(\dfrac{u - p^{k-2n}v}{p}\right) = \left(\dfrac{u}{p}\right) = 1$.

3 Symbole de Hilbert

3.1 Propriétés locales

Nous savons que $\mathbb{Q}$ se plonge dans les corps $\mathbb{R}$ et $\mathbb{Q}_p$ pour p un nombre premier et de plus son image est dense. Dès lors, pour étudier des propriétés d'objets définis sur $\mathbb{Q}$, dites globales, nous pouvons déjà mener l'étude sur les corps $\mathbb{R}$ et $\mathbb{Q}_p$, dite locale. Dans ce paragraphe nous introduisons le symbole de Hilbert et, comme nous le verrons plus loin, il joue un rôle fondamental dans le passage du local au global.

Définition 3.1.1. On dit que la forme $ax^2 + by^2 + cz^2$, où $a, b, c \in \mathbb{Q}_p$ et p est un nombre premier (resp. $a, b, c \in \mathbb{R}$) *représente 0* s'il existe $x_0, y_0, z_0 \in \mathbb{Q}_p$ (resp. $x_0, y_0, z_0 \in \mathbb{R}$) non tous nuls et tels que $ax_0^2 + by_0^2 + cz_0^2 = 0$.
Le *symbole de Hilbert* de (a, b) pour $a, b \in \mathbb{Q}_p^\times$ (resp. $a, b \in \mathbb{R}^\times$) est défini par :

$$\left(\frac{a,b}{p}\right) := \begin{cases} 1 & \text{si } ax^2 + by^2 - z^2 \text{ représente } 0 \\ -1 & \text{sinon} \end{cases}$$

$$\text{(resp.)} \left(\frac{a,b}{\infty}\right) := \begin{cases} 1 & \text{si } ax^2 + by^2 - z^2 \text{ représente } 0 \\ -1 & \text{sinon} \end{cases}$$

Notation : Dans la suite, le corps k désignera soit $\mathbb{Q}_p$, soit $\mathbb{R}$ et v sera un nombre premier ou ∞. Il est clair que $\left(\frac{a,b}{\infty}\right)$ vaut -1 si $a, b < 0$ et vaut 1 sinon.

Proposition 3.1.1. Pour $a, b, c \in k^\times$, on a les relations suivantes :

$$i) \left(\frac{a,b}{v}\right) = \left(\frac{b,a}{v}\right); \quad ii) \left(\frac{a,c^2}{v}\right) = 1; \quad iii) \left(\frac{a,-a}{v}\right) = 1; \quad iv) \left(\frac{a,1-a}{v}\right) = 1.$$

Démonstration : La formule *i)* est immédiate ; $ax^2 + by^2 - z^2$ représente 0 si et seulement si $bx^2 + ay^2 - z^2$ représente 0. Pour *ii)*, une solution non triviale de $ax^2 + (cy)^2 = z^2$ est $(0, 1, c) \in k^3$. Les formules *iii)* et *iv)* se montrent de la même manière : si $b = -a$ (resp. $b = 1 - a$), alors $ax^2 - ay^2 = z^2$ (resp. $ax^2 + (1 - a)y^2 = z^2$) a une solution non triviale $(1, 1, 0) \in k^3$ (resp. $(1, 1, 1) \in k^3$), ce qui montre *iii)* (resp. *iv)*). $\square$

Remarque : Le symbole de Hilbert de $(a, b) \in k^{\times 2}$ ne change pas si l'on multiplie a ou b par un carré de $k^\times$, il définit donc une application $\left(\frac{\cdot,\cdot}{v}\right) : k^\times/k^{\times 2} \times k^\times/k^{\times 2} \to \mathbb{F}_2 = \{\pm 1\}$.

De ce fait, les propriétés du symbole de Hilbert sur $\mathbb{Q}_p$ peuvent être établies en considérant seulement $a, b \in \mathbb{Z}_p \setminus \{0\}$ (on peut même restreindre à $a, b \in \mathbb{U} \cup p\mathbb{U}$). Nous cherchons maintenant à montrer que le symbole de Hilbert est une forme bilinéaire symétrique non dégénérée sur le $\mathbb{F}_2$-espace vectoriel $k^\times/k^{\times 2}$.

Lemme 3.1.1. Soient $a, b \in k^\times$ et $L = k[\sqrt{a}]$. Notons $N_{L/k}$ la norme associée à L/k (on rappelle que si a n'est pas un carré, $N_{L/k}(x+y\sqrt{a}) = x^2 - ay^2$) et $N_a = \{z \in k^\times \mid (\exists\, l \in L^\times) : z = N_{L/k}(l)\}$. Alors, N_a est un sous-groupe de $k^\times$ et de plus,

$$\left(\frac{a,b}{v}\right) = 1 \text{ si et seulement si } b \in N_a.$$

Démonstration : La structure de sous-groupe est immédiate, cela résulte du fait que la norme est multiplicative. Le cas où b est un carré est facile : si $b = c^2$, $b = N_{L/k}(c)$ et le symbole de Hilbert est trivial d'après la proposition précédente. On suppose que b n'est pas un carré ; si $b \in N_a$, alors il existe $x, y \in k^\times$ tels que $b = x^2 - ay^2$, de sorte que la forme $ax^2 + by^2 - z^2$ a un zéro non trivial $(y, 1, x)$ et donc $\left(\frac{a,b}{v}\right) = 1$. Réciproquement, si $ax^2 + by^2 - z^2$ représente 0, il existe $(x_0, y_0, z_0) \in k^3$ non tous nuls tels que $ax_0^2 + by_0^2 = z_0^2$. On peut supposer que a n'est pas un carré, donc en particulier $y_0 \neq 0$. Ainsi, $b = (z_0/y_0)^2 - a(x_0/y_0)^2 \in N_a$. $\square$

Lemme 3.1.2. Avec les mêmes notations que le lemme précédent,

$$(k^\times : N_a) \in \{1, 2\} \text{ et plus précisément, } N_a = k^\times \text{ si et seulement si } a \in k^{\times 2}.$$

Démonstration : Le cas $k = \mathbb{R}$ est facile à vérifier. En effet, $N_a = \{x^2 - ay^2 \neq 0 \mid x, y \in \mathbb{R}^\times\}$ $= \mathbb{R}^\times$ si $a > 0$ (*i.e* $a \in \mathbb{R}^{\times 2}$) et $N_a = \mathbb{R}_{>0} = \mathbb{R}^{\times 2}$ si $a < 0$ (*i.e* $a \notin \mathbb{R}^{\times 2}$). Dans ce dernier cas, $\mathbb{R}^\times/N_a = \mathbb{R}^\times/\mathbb{R}^{\times 2}$ est isomorphe à $\mathbb{F}_2$, avec pour représentants ± 1.

Pour $k = \mathbb{Q}_p$, commençons par traiter le cas $p = 2$:

Le groupe $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ a huit éléments et il est engendré par les classes de -1, 2 et 5. Calculons quelques symboles de Hilbert.
L'équation $ax^2 + 2y^2 = z^2$ admet des zéros non triviaux pour $a = 1$ ou -1, en effet $(x, 0, x)$ est un zéro dans le premier cas et (x, x, x) en est un dans le second. De même pour $a = 2$ ou -2, on trouve des zéros non triviaux $(x, x, 2x)$ et $(x, x, 0)$. Pour $a \in \{\pm 5, \pm 10\}$, montrons qu'il n'y a pas de solution. Par exemple pour $a = 5$, l'équation $5x^2 + 2y^2 = z^2$ est homogène et si l'on suppose l'existence d'une solution (x, y, z) non triviale, quitte à multiplier par des carrés, on peut de plus supposer que $x, y, z \in \mathbb{Z}_2$. Si $v_2(x) > 0$, alors $v_2(z) > 0$ et $v_2(y) > 0$ donc quitte à diviser par 4, on peut supposer que $v_2(x) = v_2(z) = 0$. Sous cette hypothèse, $x^2 = z^2 = 1 \pmod 8$ (les carrés modulo 8 sont 0, 1 et 4), mais la congruence $5 + 2y^2 = 1 \pmod 8$ est équivalente à $y^2 = 2 \pmod 4$, qui n'a pas de solution dans $\mathbb{Z}_2$. On traite de même les cas $a \in \{-5, \pm 10\}$:

a	1	-1	2	-2	5	-5	10	-10
$\left(\frac{a,2}{2}\right)$	1	1	1	1	-1	-1	-1	-1

Conformément à la remarque faite plus haut, le symbole de Hilbert de $(a, b) \in (\mathbb{Q}_2^\times)^2$ dépend uniquement du symbole des réprésentants des classes de a et de b modulo $\mathbb{Q}_2^{\times 2}$. D'après le lemme 3.1.1 et les calculs que nous venons d'effectuer, $\mathbb{Q}_2^\times/N_2$ est un groupe d'ordre 2, engendré par n'importe quelle classe $a\mathbb{Q}_2^{\times 2}$, où $a \in \mathbb{Q}_2^\times \backslash \mathbb{Q}_2^{\times 2}$. Pour $b \in \mathbb{Q}_2^\times \backslash \mathbb{Q}_2^{\times 2}$, des calculs similaires montrent que $\mathbb{Q}_2^\times/N_b \simeq \mathbb{F}_2$ (il suffit de considérer $b \in \{-1,-2,\pm 5,\pm 10\}$).

Pour p impair :

Si $a = c^2$ pour un certain $c \in \mathbb{Q}_p^\times$, alors tout $z \in \mathbb{Q}_p^\times$ peut s'écrire $z = x^2 - ay^2 = (x-cy)(x+cy)$, il suffit de prendre $x - cy = 1$ et $x + cy = z$, $i.e$ $x = \frac{z+1}{2}$ et $y = \frac{z-1}{2c}$. Ainsi, si a est un carré, alors $N_a = \mathbb{Q}_p^\times$. Il reste à montrer la réciproque, supposons par l'absurde que $N_a = \mathbb{Q}_p^\times$ et $a \in \mathbb{Q}_p^\times \backslash \mathbb{Q}_p^{\times 2}$. On commence par traiter le cas où $a \in \mathbb{U}$: s'il existe $z \in \mathbb{U}$ tel que $\left(\dfrac{a,pz}{p}\right) = 1$, alors $pz \in N_a$ et par symétrie du symbole de Hilbert, $a \in N_{pz}$, donc il existe $x, y \in \mathbb{Q}_p^\times$ tels que $a = x^2 - pzy^2$. Or, $0 = v_p(a) = \min\{2v_p(x); 2v_p(y)+1\}$, donc $v_p(x) = 0$ et $v_p(y) \geq 0$. La réduction modulo p donne alors $a = x^2 \pmod p$, $i.e$ $\left(\dfrac{a}{p}\right) = 1$. Posons $f \in \mathbb{Z}_p[X]$ le polynôme défini par $f(X) = X^2 - a$, on vient de voir que $f(x) = 0 \pmod p$ et comme $f'(x) = 2x$ et p est impair, d'après le lemme de Hensel 2.3.2, le zéro modulo p se relève en un zéro dans $\mathbb{Z}_p$. Ceci est absurde, puisqu'on a supposé que a n'est pas un carré. On en déduit que pour tout $z \in \mathbb{U}$, $\left(\dfrac{a,pz}{p}\right) = -1$, donc en particulier $N_a \neq \mathbb{Q}_p^\times$. Le cas où $a \in p\mathbb{U}$ se ramène au cas que nous venons de traiter ; on peut écrire $a = pz$ avec $z \in \mathbb{U}$. En choisissant $b \in \mathbb{U}$ tel que $\left(\dfrac{b}{p}\right) = -1$, alors $\left(\dfrac{a,b}{p}\right) = \left(\dfrac{b,pz}{p}\right) = -1$, donc $N_a \neq \mathbb{Q}_p^\times$. Puisque le symbole de Hilbert ne dépend que des classes des éléments de $\mathbb{Q}_p^\times$ modulo les carrés, le cas $a \in \mathbb{U} \cup p\mathbb{U}$ est suffisant pour établir le résultat.

On a terminé la démonstration de l'équivalence, il reste à calculer l'indice de N_a dans $\mathbb{Q}_p^\times$:

D'après le corollaire 2.4.2 le groupe $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ est d'ordre 4 et pour prouver que l'indice de N_a dans $\mathbb{Q}_p^\times$ vaut 1 ou 2, il suffit de montrer que N_a contient strictement les carrés de $\mathbb{Q}_p^\times$. On peut supposer que $p^2 \nmid a$ ($i.e$ $v_p(a) \in \{0,1\}$) et que a n'est pas un carré (ce cas a déjà été traité). On distingue alors deux cas.
Si $v_p(a) = 0$ et si $u \in \mathbb{U}$, alors l'image modulo p de la forme $x^2 - ay^2 - uz^2$ est de rang 3 sur $\mathbb{F}_p$. D'après le corollaire 1.1.2 du théorème de Chevalley-Warning , il existe un vecteur isotrope non trivial $v_0 = (x_0, y_0, z_0) \in (\mathbb{F}_p)^3$. Comme $p \nmid 2$, on peut appliquer le lemme d'Hensel 2.3.2 pour relever v_0 en un vecteur isotrope $v_1 = (x_1, y_1, z_1) \in (\mathbb{Z}_p)^3$ non trivial de la forme de départ. De plus, $z_1 \neq 0$ car sinon a serait un carré ; on en conclut que $u \in N_a$. En appliquant ceci à un élément u de $\mathbb{U}$ qui n'est pas un carré dans $\mathbb{U}$ (et donc dans $\mathbb{Q}_p^\times$), on a bien prouvé $\mathbb{Q}_p^{\times 2} \subsetneq N_a$ (il en existe forcément car $p \geq 3$ et les éléments de $\mathbb{F}_p^\times$ définissent des unités p-adiques distinctes mais seulement $(p-1)/2$ d'entre eux sont des carrés).
Si $v_p(a) = 1$, alors $N_{L/k}(\sqrt{a}) = -a \in N_a$. Or, $-a$ ne peut être un carré dans $\mathbb{Q}_p^\times$, puisque sa valuation vaut 1. □

Théorème 3.1.1. *Le symbole de Hilbert* $\left(\dfrac{\cdot,\cdot}{v}\right) : k^\times/k^{\times 2} \times k^\times/k^{\times 2} \to \mathbb{F}_2 = \{\pm 1\}$ *est une forme bilinéaire symétrique et non dégénérée.*

Démonstration : Soient $a, b, b' \in k^\times$, la linéarité en la deuxième variable s'exprime par

$\left(\frac{a,bb'}{v}\right) = \left(\frac{a,b}{v}\right)\left(\frac{a,b'}{v}\right)$. On a plusieurs cas à distinguer :

- Si $\left(\frac{a,b}{v}\right) = \left(\frac{a,b'}{v}\right) = 1$, *i.e* $b,b' \in N_a$, alors $bb' \in N_a$ donc $\left(\frac{a,bb'}{v}\right) = 1$.
- Si $\left(\frac{a,b}{v}\right) = 1$ et $\left(\frac{a,b'}{v}\right) = -1$, alors $\left(\frac{a,bb'}{v}\right) = -1$. En effet, si $\left(\frac{a,bb'}{v}\right) = 1$, alors $\left(\frac{a,b'}{v}\right) = \left(\frac{a,b^2b'}{v}\right) = \left(\frac{a,b}{v}\right)\left(\frac{a,bb'}{v}\right) = 1$, contradiction.

- Si $\left(\frac{a,b}{v}\right) = \left(\frac{a,b'}{v}\right) = -1$, alors d'après le lemme 3.1.2, a n'est pas un carré et b,b' ont la même classe dans $k^\times/N_a$. Puisque ce groupe est d'ordre 2, il existe $c \in N_a$ tel que $bb' = c$. Ainsi, $\left(\frac{a,bb'}{v}\right) = 1 = (-1)^2 = \left(\frac{a,b}{v}\right)\left(\frac{a,b'}{v}\right)$.

La symétrie du symbole de Hilbert montrée dans la proposition 3.1.1 assure la linéarité en l'autre variable. On a bien démontré que le symbole de Hilbert est une forme bilinéaire symétrique sur le $\mathbb{F}_2$-espace vectoriel $k^\times/k^{\times 2}$. Enfin, si $\left(\frac{a,b}{v}\right) = 1$ pour tout $b \in k^\times$, alors d'après le lemme 3.1.2, $a \in k^{\times 2}$, ce qui prouve que la forme est non dégénérée. □

Le prochain résultat permet de calculer explicitement des symboles de Hilbert ; pour cela on étend le symbole de Legendre aux entiers p-adiques en posant pour $u \in \mathbb{U}$, $\left(\frac{u}{p}\right) = 1$ si u est un carré dans $\mathbb{Z}_p$ et -1 sinon.

Théorème 3.1.2. *Soient p premier impair et $m,n \in \mathbb{Q}_p^\times$. On pose $a = v_p(m)$ et $b = v_p(n)$, de sorte que $m^b/n^a = r/s$, avec $r,s \in \mathbb{U}$. Alors,*

$$\left(\frac{m,n}{p}\right) = \left(\frac{(-1)^{ab}rs}{p}\right).$$

Démonstration : On commence par remarquer que si $m = m_1m_2$ avec $m_1,m_2 \in \mathbb{Q}_p^\times$, alors en définissant de même $a_1 = v_p(m_1)$, $a_2 = v_p(m_2)$, $m_1^b/n^{a_1} = r_1/s_1$ et $m_2^b/n^{a_2} = r_1/s_1$, on obtient $a = a_1 + a_2$ et $r/s = r_1r_2/s_1s_2$, donc si la relation est vraie pour m_1 et m_2, elle est aussi vraie pour m car :

$$\left(\frac{m,n}{p}\right) = \left(\frac{m_1,n}{p}\right)\left(\frac{m_2,n}{p}\right) = \left(\frac{(-1)^{a_1b}r_1s_1}{p}\right)\left(\frac{(-1)^{a_2b}r_2s_2}{p}\right) = \left(\frac{(-1)^{ab}rs}{p}\right).$$

Cette observation nous permet de réduire les cas à considérer ; il suffit de montrer :

$$i)\ \left(\frac{p,p}{p}\right) = \left(\frac{-1}{p}\right),\quad ii)\ \left(\frac{p,n}{p}\right) = \left(\frac{n,p}{p}\right) = \left(\frac{n}{p}\right) \text{ si } p \nmid n,\quad iii)\ \left(\frac{m,n}{p}\right) = 1 \text{ si } p \nmid mn.$$

Le cas $i)$ se ramène à $ii)$ via $\left(\frac{p,p}{p}\right) = \left(\frac{-p,p}{p}\right)\left(\frac{-1,p}{p}\right) = \left(\frac{-1,p}{p}\right)$.
Montrons $ii)$: il s'agit de prouver que $px^2 + ny^2 - z^2$ a une solution si et seulement si

$\left(\frac{n}{p}\right) = 1$. On suppose qu'il existe $x, y, z \in \mathbb{Q}_p^\times$ tels que $px^2 + ny^2 = z^2$. Quitte à multiplier ou diviser par p^2, on peut supposer que $x, y, z \in \mathbb{Z}_p$ et que $p \nmid y$ (sinon on aurait $p \mid z$ donc $p \mid x$ et on pourrait simplifier par p). En réduisant modulo p, $ny^2 = z^2 \pmod p$, donc $n = (zy^{-1})^2 \pmod p$, d'où $\left(\frac{n}{p}\right) = 1$. Réciproquement, si n est un carré modulo p, on écrit $n = {z_0}^2 \pmod p$. Par le lemme de Hensel 2.3.2, le zéro de $f(X) = X^2 - n$ modulo p se relève en un zéro dans $\mathbb{Z}_p$: $n = z^2$ avec $z \in \mathbb{Z}_p$. Il suit que $(0, 1, z)$ est un zéro non trivial de $px^2 + ny^2 - z^2$.

Si $p \nmid mn$, alors $a = b = 0$ et le membre de droite de *iii)* vaut $\left(\frac{1}{p}\right) = 1$. On s'occupe du membre de gauche ; toujours en appliquant le lemme de Hensel 2.3.2, il suffit de montrer l'existence d'une solution de $mx^2 + ny^2 = z^2 \pmod p$. Posons $g : \mathbb{F}_p \to \mathbb{F}_p$, $(y \mapsto m(1 - ny^2))$, alors $g(y) = g(y') \Leftrightarrow y^2 = y'^2$ (car m, n sont inversibles modulo p), donc g prend $(p+1)/2$ valeurs, dont au moins une est un carré dans $\mathbb{F}_p$; notons $m(1 - n{y_0}^2) = X^2 \pmod p$. Comme $p \nmid m$, on peut choisir x_0 tel que $X = mx_0 \pmod p$, donc $m{x_0}^2 = (1 - n{y_0}^2) \pmod p$ et l'équation $mx^2 + ny^2 = z^2 \pmod p$ a une solution $(x_0, y_0, 1)$. $\square$

Pour $p = 2$, le résultat suivant donne des expressions du symbole de Legendre sur $\mathbb{Q}_2$.

Théorème 3.1.3. *Soient $m, n \in \mathbb{Q}_2^\times$, il existe $a, b \in \mathbb{Z}$ et $u, v \in \mathbb{U}$ tels que $m = 2^a u$ et $n = 2^b v$. Alors,*

$$\left(\frac{2, m}{2}\right) = (-1)^{\frac{\bar{u}^2 - 1}{8}} \quad \text{et} \quad \left(\frac{m, n}{2}\right) = (-1)^{\frac{(\bar{u}-1)(\bar{v}-1)}{4}},$$

où $\bar{u}, \bar{v} \in \{0, \dots, 7\}$ sont les entiers correspondants aux réductions modulo $\mathbb{U}_3 = 1 + 8\mathbb{Z}_2$ de u et de v.

Démonstration : On montre la première égalité. Dans la démonstration du lemme 3.1.2 on a vu que $\left(\frac{2, 2}{2}\right) = 1$, donc en utilisant la linéarité, $\left(\frac{2, m}{2}\right) = \left(\frac{2, 2^a u}{2}\right) = \left(\frac{2, u}{2}\right)$. De plus, si $u = 1 \pmod 8$, alors u est un carré dans $\mathbb{Q}_2^\times$ donc $\left(\frac{2, u}{2}\right) = 1$. Il suit que le symbole $\left(\frac{2, u}{2}\right)$ ne dépend que de la classe de u modulo $\mathbb{U}_3$. Or, $\{\pm 1; \pm 5\}$ est un système de représentants de $\mathbb{U}/\mathbb{U}_3$ et on vérifie alors que le membre de droite coïncide avec les résultats trouvés dans la démonstration du lemme 3.1.2 :

a	1	-1	5	-5
$\left(\frac{a, 2}{2}\right)$	1	1	-1	-1

Montrons la deuxième égalité ; le même raisonnement nous invite à considérer seulement $u, v \in \{1, 3, 5, 7\}$. Après calcul, le membre de droite coïncide avec les symboles :

$u \diagdown v$	1	3	5	7
1	1	1	1	1
3	1	-1	1	-1
5	1	1	1	1
7	1	-1	1	-1

$\square$

3.2 Propriétés globales

Dans ce paragraphe, $\mathcal{V}$ désigne la réunion de tous les nombres premiers et de ∞.

Théorème 3.2.1. *(formule du produit) Soient $a, b \in \mathbb{Q}^\times$, alors $\left(\frac{a,b}{v}\right) = 1$ pour presque tout $v \in \mathcal{V}$ et de plus,*

$$\prod_{v \in \mathcal{V}} \left(\frac{a,b}{v}\right) = 1.$$

Démonstration : Comme le symbole de Hilbert est bilinéaire, on est amené à considérer seulement les cas où a, b sont ± 1 ou des nombres premiers. En appliquant les deux théorèmes précédents, on montre que dans tous les cas les facteurs non triviaux se compensent :
1) Pour $a = b = -1$, on a $\left(\frac{-1,-1}{\infty}\right) = \left(\frac{-1,-1}{2}\right) = -1$ et $\left(\frac{-1,-1}{p}\right) = 1$ pour p impair.
2) Pour $a = -1$ et $b = q$, avec q premier. Si $q = 2$, on a $\left(\frac{-1,2}{v}\right) = 1$ pour tout $v \in \mathcal{V}$ (c'est clair pour $v = 2$ ou ∞, et pour v premier impair cela résulte de $iii)$ dans la démonstration du théorème 3.1.2, car $v \nmid -2$). Si q est impair, on a $\left(\frac{-1,q}{v}\right) = 1$ pour tout $v \notin \{2, q\}$ (c'est évident pour $v = \infty$ et pour p premier impair c'est d'après $iii)$ du théorème 3.1.2, car $p \nmid -q$). D'une part, $\left(\frac{-1,q}{2}\right) = -1^{\frac{(-1-1)(q-1)}{4}} = (-1)^{\frac{q-1}{2}}$ (avec $u = -1$ et $v = q$ dans le théorème 3.1.3). D'autre part, $\left(\frac{-1,q}{q}\right) = \left(\frac{(-1)^0 - 1}{q}\right) = (-1)^{\frac{q-1}{2}}$ (avec $m = -1$, $n = q$, $a = 0$ et $b = 1$ dans le théorème 3.1.2).
3) Si $a = q$, $b = q'$ sont deux nombres premiers ; le cas $q = q'$ se ramène au précédent car $\left(\frac{q,q}{v}\right) = \left(\frac{-1,q}{v}\right)$, pour tout $v \in \mathcal{V}$. Si $q \neq q'$ et $q' = 2$, on a $\left(\frac{q,2}{v}\right) = 1$ pour tout $v \notin \{2, q\}$ (toujours d'après $iii)$ du théorème 3.1.2) et $\left(\frac{q,2}{q}\right) = \left(\frac{2}{q}\right) = \left(\frac{q,2}{2}\right)$ (d'après $ii)$ du théorème 3.1.2 et la première relation du théorème 3.1.3). Enfin, si $q \neq q'$ et $q, q' \neq 2$, alors $\left(\frac{q,q'}{v}\right) = 1$ pour tout $v \notin \{2, q, q'\}$ et $\left(\frac{q,q'}{2}\right) = (-1)^{\frac{(\bar{q}-1)(\overline{q'}-1)}{4}}$, d'après le théorème 3.1.3. Le théorème 3.1.2 donne $\left(\frac{q,q'}{q}\right) = \left(\frac{q'}{q}\right)$ et $\left(\frac{q,q'}{q'}\right) = \left(\frac{q}{q'}\right)$. Or d'après la loi de réciprocité quadratique, $\left(\frac{q'}{q}\right)\left(\frac{q}{q'}\right) = (-1)^{\frac{(\bar{q}-1)(\overline{q'}-1)}{4}}$.

On a bien montré que dans tous les cas, $\left(\frac{a,b}{v}\right) = 1$ sauf pour un nombre fini de $v \in \mathcal{V}$ et la formule du produit est toujours vérifiée :

$$\prod_{v \in \mathcal{V}} \left(\frac{a,b}{v}\right) = 1.$$

$\square$

Remarque : Nous venons de voir que la loi de réciprocité quadratique 1.2.2 implique la formule du produit 3.2.1, en fait il y a équivalence entre les deux : si a, b sont des nombres premiers impairs, les facteurs non triviaux du produit ($i.e$ lorsque le symbole vaut -1) sont pour $v \in \{2, a, b\}$. Or, les théorèmes 3.1.2 et 3.1.3 permettent de calculer ces symboles de Hilbert et la loi de réciprocité quadratique 1.2.2 en découle immédiatement,

$$\left(\frac{a,b}{2}\right)\left(\frac{a,b}{a}\right)\left(\frac{a,b}{b}\right) = 1 \Rightarrow \left(\frac{b}{a}\right)\left(\frac{a}{b}\right) = \left(\frac{a,b}{2}\right) = (-1)^{\frac{(\bar{a}-1)(\bar{b}-1)}{4}}.$$

L'intérêt du symbole de Hilbert est qu'il se généralise aux corps de nombres algébriques ; l'ensemble $\mathcal{V}$ est alors l'ensemble des « places » du corps de nombres.

Le résultat suivant donne une condition d'existence de rationnels de symboles de Hilbert donnés.

Théorème 3.2.2. *Soient I un ensemble fini, $(a_i)_{i\in I}$ une famille d'éléments de $\mathbb{Q}^\times$ et soit $(\varepsilon_{i,v})_{(i,v)\in I\times\mathcal{V}}$ une famille de nombres égaux à ± 1. Pour qu'il existe $x \in \mathbb{Q}^\times$ tel que $\left(\frac{a_i, x}{v}\right) = \varepsilon_{i,v}$ pour tout $i \in I$ et tout $v \in \mathcal{V}$, il faut et il suffit que les trois conditions suivantes soient satisfaites :*
i) Presque tous les $\varepsilon_{i,v}$ sont égaux à 1.
ii) Pour tout $i \in I$, on a $\prod_{v\in\mathcal{V}} \varepsilon_{i,v} = 1$.
iii) Pour tout $v \in \mathcal{V}$, il existe $x_v \in \mathbb{Q}_v^\times$ tel que

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

pour tout $i \in I$ et avec la convention $\mathbb{Q}_\infty^\times = \mathbb{R}^\times$.

Démonstration : La condition est clairement nécessaire ; s'il existe un tel $x \in \mathbb{Q}^\times$, alors à i fixé,

$$\prod_{v\in\mathcal{V}} \left(\frac{a_i, x}{v}\right) = \prod_{v\in\mathcal{V}} \varepsilon_{i,v} = 1,$$

et seulement un nombre fini de $\varepsilon_{i,v}$ sont non triviaux. On vient de montrer ii) et i), et pour iii) il suffit de prendre $x_v = x$ pour tout $v \in \mathcal{V}$. La réciproque est bien plus difficile et nous aurons besoin de deux résultats :

Théorème 3.2.3. *[de la progression arithmétique] (Dirichlet, 1837)*
Si $a, m \in \mathbb{N}_{>0}$ sont des entiers premiers entre eux, alors il existe une infinité de nombres premiers p tels que $p = a \pmod m$.

Ce théorème est hautement non trivial et nous l'admettrons.

Lemme 3.2.1. (d'approximation) Soit S une partie finie de $\mathcal{V}$. L'image de $\mathbb{Q}$ dans $\prod_{v\in S} \mathbb{Q}_v$ est dense dans ce produit, pour la topologie produit.

Démonstration (du lemme) : Quitte à agrandir S, on peut supposer que $S = \{\infty, p_1, \dots, p_n\}$, où les p_i sont des nombres premiers distincts. Soit $(x_\infty, x_1, \dots, x_n) \in \mathbb{R} \times \mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_n}$, montrons que ce point est adhérent à l'image de $\mathbb{Q}$ dans $\mathbb{R} \times \mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_n}$. Quitte à faire une homothétie de rapport entier, on peut supposer que l'on a $x_i \in \mathbb{Z}_{p_i}$ pour tout i $\in \{1, \dots, n\}$. Montrons :

$$(\forall \varepsilon > 0)\,(\forall N \in \mathbb{N})\,(\exists x \in \mathbb{Q}) \begin{cases} |x - x_\infty| < \varepsilon \\ \forall i \in \{1, \dots, n\},\ v_{p_i}(x - x_i) \geq N \end{cases}.$$

Soient $\varepsilon > 0$, $N \geq 0$ et pour $i \in \{1, \dots, n\}$, posons $m_i = p_i^N$ et $m = \prod_i m_i$. D'après le théorème chinois, et puisque les m_i sont deux à deux premiers entre eux, le système :

$$\begin{cases} x = x_1 & \pmod{m_1} \\ \vdots & \vdots \\ x = x_n & \pmod{m_n} \end{cases}$$

a une solution $x_0 \in \mathbb{Z}$ (qui vérifie $v_{p_i}(x_0 - x_i) \geq N$ pour tout $i \in \{1, \dots, n\}$, par construction). Soit q un nombre premier distinct de $p_1, \dots, p_n$, posons $A := \{a/q^m \,|\, a \in \mathbb{Z},\, m \in \mathbb{N}\}$. Alors A est dense dans $\mathbb{R}$. En effet, il suffit de montrer que A est dense dans $[0\,;1]$; cela provient du développement en base q. Ainsi, il existe un rationnel $u = a/q^m$ tel que :

$$|x_0 - x_\infty + u p_1^N \cdots p_n^N| < \varepsilon$$

Le rationnel $x = x_0 + u p_1^N \cdots p_n^N$ convient :

$$v_{p_i}(x_0 - x_i) \geq \min\{v_{p_i}(x_0 - x_i)\,;\, v_{p_i}(u p_1^N \cdots p_n^N)\} \geq N,\ \text{pour tout } i \in \{1, \dots, n\}.$$

La deuxième inégalité est vraie car $q \nmid p_i \Rightarrow v_{p_i}(u p_i^N) \geq N$. □

Revenons à la démonstration du théorème :
Soit $(\varepsilon_{i,v})_{(i,v) \in I \times \mathcal{V}}$ une famille de nombres égaux à ± 1 et satisfaisant $i)$, $ii)$ et $iii)$. Quitte à multiplier les a_i par le carré d'un entier (ne change pas le symbole de Hilbert), on peut supposer que les a_i sont des entiers. Soit S le sous-ensemble formé de 2, ∞, et des facteurs premiers des a_i. Soit T le sous-ensemble des $v \in \mathcal{V}$ tels qu'il existe $i \in I$ avec $\varepsilon_{i,v} = -1$. Ce sont deux ensembles finis (d'après le théorème 3.2.1 pour T).

Premier cas : Si $S \cap T = \emptyset$, posons :

$$a := \prod_{v \in T \setminus \{\infty\}} v \quad \text{et} \quad m := 8 \prod_{v \in S \setminus \{2, \infty\}} v.$$

Par hypothèse, $S \cap T = \emptyset$, donc a et m sont premiers entre eux et d'après le théorème de la progression arithmétique 3.2.3, il existe un nombre premier $q = a \pmod m$ tel que $q \notin S \cup T$ (c'est un ensemble fini). On va montrer que $x = aq$ convient, c'est-à-dire que $\left(\dfrac{a_i, x}{v}\right) = \varepsilon_{i,v}$, pour tout $i \in I$ et tout $v \in \mathcal{V}$.

Si $v \in S$, on a $v \in \mathcal{V} \setminus T$, donc $\varepsilon_{i,v} = 1$ et il faut vérifier que $\left(\dfrac{a_i, x}{v}\right) = 1$.

Si $v = \infty$, on a bien $\left(\dfrac{a_i, x}{\infty}\right) = 1$, puisque $x > 0$. Si $v = p$ est un nombre premier, on a $x = aq = a^2 \pmod m$, d'où $x = a^2 \pmod 8$ si $p = 2$, et $x = a^2 \pmod p$ si $p \neq 2$ (car $p \in S$). Dans les deux cas, les images de x et de a dans $\mathbb{Q}_p^\times$ sont des unités p-adiques (x et a sont des entiers et $p \nmid aq$, car $p \notin T$ et $q \notin S \cup T$), donc x est un carré dans $\mathbb{Q}_p^\times$ (d'après le théorème 2.4.2) et on a bien $\left(\dfrac{a_i, x}{v}\right) = 1$.

Si $v = p \notin S$, alors $p \nmid a_i$ donc l'image de a_i est une unité p-adique. Comme $p \neq 2 \in S$ et $v_p(a_i) = 0$, on a d'après le théorème 3.1.2 et en utilisant la multiplicativité du symbole de Legendre :

$$\left(\frac{a_i, n}{p}\right) = \left(\frac{a_i}{p}\right)^{v_p(n)}, \quad \text{pour tout } n \in \mathbb{Q}_p^\times.$$

Si $p \notin T \cup \{q\}$, l'image de x est une unité p-adique, d'où $v_p(x) = 0$ et la formule ci-dessus montre que $\left(\dfrac{a_i, x}{p}\right) = 1$; de plus comme $p \notin T$, on a $\varepsilon_{i,p} = 1$.

Si $p \in T$, on a $v_p(x) = 1$; d'autre part, la condition iii) donne l'existence d'un $x_p \in \mathbb{Q}_p^\times$ tel que $\left(\dfrac{a_i, x_p}{p}\right) = \varepsilon_{i,p}$, pour tout $i \in I$. Comme $p \in T$, l'un des $\varepsilon_{i,p}$ est égal à -1 et donc $v_p(x_p)$ est impair (sinon x_p serait un carré de $\mathbb{Q}_p^\times$ et tous les symboles de Hilbert seraient triviaux). Donc $v_p(x) = 1 \pmod 2$ et d'après la formule ci-dessus,

$$\left(\frac{a_i, x}{p}\right) = \left(\frac{a_i}{p}\right) = \left(\frac{a_i, x_p}{p}\right) = \varepsilon_{i,p}, \ \text{pour tout } i \in I.$$

Il reste à considérer le cas $p = q$: on se ramène alors aux autres cas grâce à la réciprocité du symbole Hilbert :

$$\left(\frac{a_i, x}{q}\right) = \prod_{v \neq q} \left(\frac{a_i, x}{v}\right) = \prod_{v \neq q} \varepsilon_{i,v} = \varepsilon_{i,q}.$$

Ceci achève la démonstration dans le cas $S \cap T = \emptyset$.

Cas général : On sait que les carrés de $\mathbb{Q}_v^\times$ forment un sous-groupe ouvert de $\mathbb{Q}_v^\times$. Si l'on fixe $z_v \in \mathbb{Q}_v^\times$ et $V_v \subset \mathbb{Q}_v^{\times 2}$ un voisinage de z_v^2 pour tout $v \in S$, alors d'après le lemme d'approximation 3.2.1, il existe $x' \in \mathbb{Q}$ tel que $x'/x_v \in V_v$ pour tout $v \in S$. Ainsi, pour tout $v \in S$, x'/x_v est un carré dans $\mathbb{Q}_v^\times$ et en particulier,

$$\begin{aligned} 1 = \left(\frac{a_i, \frac{x'}{x_v}}{v}\right) &\Rightarrow 1 = \left(\frac{a_i, \frac{x'}{x_v} x_v^2}{v}\right) \\ &\Rightarrow 1 = \left(\frac{a_i, x'}{v}\right)\left(\frac{a_i, x_v}{v}\right) \\ &\Rightarrow \left(\frac{a_i, x'}{v}\right) = \left(\frac{a_i, x_v}{v}\right) \ \left(= \varepsilon_{i,v}\right) \end{aligned}$$

Si l'on pose $\eta_{i,v} = \varepsilon_{i,v} \left(\dfrac{a_i, x'}{v}\right)$, la famille $(\eta_{i,v})_{(i,v) \in I \times \mathcal{V}}$ vérifie les conditions i), ii) et iii). En effet, presque tous les $\varepsilon_{i,v}$ sont égaux à 1 par hypothèse et presque tous les $\left(\dfrac{a_i, x'}{v}\right)$ le sont aussi, d'après le théorème 3.2.1, ce qui prouve i). Pour ii) : soit $i \in I$, on a $\prod_{v \in \mathcal{V}} \eta_{i,v} = 1$, par hypothèse et d'après le théorème 3.2.1. Par hypothèse, pour tout $v \in \mathcal{V}$, il existe $x_{\sqsubseteq} \in \mathbb{Q}_v^\times$ tel que $\left(\dfrac{a_i, x_v}{v}\right) = \varepsilon_{i,v}$, pour tout $i \in I$. Il est clair qu'en prenant $x'_v = x' x_v \in \mathbb{Q}_v^\times$, on a $\left(\dfrac{a_i, x'_v}{v}\right) = \eta_{i,v}$, pour tout $i \in I$, ce qui prouve iii). De plus on a $\eta_{i,v} = 1$ si $v \in S$, donc $S \cap T = \emptyset$ (le T ici correspond aux $\eta_{i,v}$). On a prouvé que dans ce cas il existe $y \in \mathbb{Q}^\times$ tel que :

$$\left(\frac{a_i, y}{v}\right) = \eta_{i,v}, \text{ pour tout } (i, v) \in I \times \mathcal{V}.$$

Si l'on prend $x = yx'$, alors x répond à la question :

$$\left(\frac{a_i, x}{v}\right) = \left(\frac{a_i, yx'}{v}\right) = \left(\frac{a_i, y}{v}\right)\left(\frac{a_i, x'}{v}\right) = (\eta_{i,v})^2 \varepsilon_{i,v} = \varepsilon_{i,v},$$

pour tout $(i, v) \in I \times \mathcal{V}$. Ce qui achève la démonstration et notre étude du symbole de Hilbert.
$\square$

4 Classification des formes quadratiques sur $\mathbb{Q}$

Dans toute cette section, p est un nombre premier et (V, q) est un espace quadratique non dégénéré sur le corps $k = \mathbb{Q}_p$.

4.1 Vers un système complet d'invariants

Soit $n \in \mathbb{N}_{>0}$ le rang de (V, q), son discriminant $\operatorname{disc}(q)$ est un élément de $k^\times/k^{\times 2}$. Nous ferons l'abus de noter un élément de $k^\times$ et sa classe modulo $k^{\times 2}$ par la même lettre.

Définition 4.1.1. Soient $e = (e_1, \dots, e_n)$ une base orthogonale de V et $a_i = q(e_i) \in k^\times$ pour tout $1 \leq i \leq n$. On note $\varepsilon(e)$ l'entier égal à ± 1 et défini par :

$$\varepsilon(e) := \prod_{1 \leq i < j \leq n} \left(\frac{a_i, a_j}{p} \right).$$

L'intérêt est que ce nombre est un invariant au sens suivant :

Théorème 4.1.1. *L'entier $\varepsilon(e)$ ne dépend pas de la base orthogonale e.*

Démonstration : Soit e une base orthogonale de V. Si $n = 1$, le produit est indexé par l'ensemble vide et on a $\varepsilon(e) = 1$ par convention. Si $n = 2$, on a $\varepsilon(e) = 1$ si et seulement si $\left(\frac{a_1, a_2}{p} \right) = 1$, si et seulement si la forme $a_1 x^2 + a_2 y^2 - z^2$ représente 0. D'après le corollaire 1.3.1, cela équivaut au fait que la forme $a_1 x^2 + a_2 y^2$ représente 1, c'est-à-dire qu'il existe $x \in V$ tel que $q(x) = 1$, et cela ne dépend pas de la base. Soit $n \geq 3$, on raisonne par récurrence ; d'après le théorème 1.3.3, il suffit de montrer que $\varepsilon(e) = \varepsilon(e')$ pour deux bases e et e' contiguës. Quitte à permuter les vecteurs de e' (cela ne change pas la valeur de $\varepsilon(e')$ car le symbole de Hilbert est symétrique), on peut supposer que $e' = (e'_1, \dots, e'_n)$ avec $e'_1 = e_1$. Si pour tout $1 \leq i \leq n$, le scalaire a'_i désigne $q(e'_i)$, on a $a_1 = a'_1$ et par bilinéarité du symbole de Hilbert :

$$\begin{aligned} \varepsilon(e) &= \left(\frac{a_1, a_2 \cdots a_n}{p} \right) \prod_{2 \leq i < j} \left(\frac{a_i, a_j}{p} \right) \\ &= \left(\frac{a_1, \operatorname{disc}(q)\, a_1}{p} \right) \prod_{2 \leq i < j} \left(\frac{a_i, a_j}{p} \right), \end{aligned}$$

où l'on a utilisé les propriétés du symbole de Hilbert et le fait que $\operatorname{disc}(q) = a_1 \cdots a_n$. De même, $\varepsilon(e') = \left(\frac{a_1, \operatorname{disc}(q)\, a_1}{p} \right) \prod_{2 \leq i < j} \left(\frac{a'_i, a'_j}{p} \right)$. Si V' désigne l'orthogonal $e_1^\perp$, l'hypothèse de récurrence appliquée à $(V', q_{|V'})$ (de dimension $n - 1$) permet de conclure que $\prod_{2 \leq i < j} \left(\frac{a_i, a_j}{p} \right) = \prod_{2 \leq i < j} \left(\frac{a'_i, a'_j}{p} \right)$. Ceci achève la récurrence et la démonstration. $\square$

Définition 4.1.2. Le théorème 4.1.1 permet de définir le *symbole de Hilbert de* q, noté $\varepsilon(q)$ et défini comme étant égal à $\varepsilon(e)$, où e est une base orthogonale quelconque. Les nombres $\operatorname{disc}(q)$ et $\varepsilon(q)$ sont des invariants au sens suivant :
Si q est une forme à n variables et équivalente à $a_1x_1^2 + \cdots + a_nx^2$, alors $\operatorname{disc}(q) = a_1 \cdots a_n \in k^\times/k^{\times 2}$ et $\varepsilon(q) = \prod_{1\leq i<j\leq n} \left(\dfrac{a_i, a_j}{p}\right) \in \{\pm 1\}$ sont des invariants de la classe d'équivalence de q.

On cherche maintenant à donner une condition nécessaire et suffisante pour qu'une forme représente un élément de k. Commençons par un rappel sur le $\mathbb{F}_2$-espace vectoriel $k^\times/k^{\times 2}$: on a vu que $k^\times/k^{\times 2}$ a 4 éléments (resp. 8 éléments) si $p \neq 2$ (resp. si $p = 2$). Dans tous les cas, ce cardinal sera noté 2^r, avec $r = 2$ ou $r = 3$. Dans la suite on notera $d(q)$ plutôt que $\operatorname{disc}(q)$ pour désigner le discriminant de la forme quadratique q.

Lemme 4.1.1. Soient $a \in k^\times/k^{\times 2}$ et $\varepsilon \in \{\pm 1\}$, on note $H_a^\varepsilon := \left\{x \in k^\times/k^{\times 2} \mid \left(\dfrac{x, a}{p}\right) = \varepsilon\right\}$. Si $a = 1$, H_a^1 a 2^r éléments et H_a^{-1} est vide. Si $a \neq 1$, alors H_a^1 et H_a^{-1} ont tous deux pour cardinal 2^{r-1}. De plus, si $a, a' \in k^\times/k^{\times 2}$ et $\varepsilon, \varepsilon' \in \{\pm 1\}$ sont tels que $H_a^\varepsilon, H_{a'}^{\varepsilon'} \neq \emptyset$, alors $H_a^\varepsilon \cap H_{a'}^{\varepsilon'} = \emptyset$ si et seulement si $a = a'$ et $\varepsilon\varepsilon' = -1$.

Démonstration : La première assertion est évidente pour $a = 1$. Si $a \neq 1$, on considère le morphisme de $\mathbb{F}_2$-espaces vectoriels $k^\times/k^{\times 2} \to \{\pm 1\}$; $b \mapsto \left(\dfrac{a, b}{p}\right)$; comme $a \neq 1$ le morphisme est surjectif et son noyau H_a^1 est un hyperplan de $k^\times/k^{\times 2}$ et a 2^{r-1} éléments. Son complémentaire H_a^{-1} a également 2^{r-1} éléments. Maintenant si H_a^ε et $H_{a'}^{\varepsilon'}$ sont non vides et disjoints, ils ont nécessairement 2^{r-1} éléments chacun et sont complémentaires l'un de l'autre. On en déduit $H_a^\varepsilon = H_{a'}^{-\varepsilon'}$. Si $\varepsilon = \varepsilon'$, quitte à prendre les complémentaires on trouve $H_a^1 = H_{a'}^{-1}$, mais il est clair que $1 \in H_a^1 \cap H_{a'}^1$, donc $H_{a'}^1$ et $H_{a'}^{-1}$ ne sont pas disjoints, contradiction. Ainsi, $\varepsilon \neq \varepsilon'$ et en prenant les complémentaires, $H_a^1 = H_{a'}^1$ et $H_a^{-1} = H_{a'}^{-1}$ donc :

$$\left(\frac{x, a'}{p}\right) = \left(\frac{x, a'}{p}\right), \text{ pour tout } x \in k^\times/k^{\times 2}$$

Puisque le symbole de Hilbert est non dégénéré, on en déduit $a = a'$ et évidemment $\varepsilon = -\varepsilon'$. La réciproque est triviale. $\square$

Le résultat suivant est important ; on montre que toute forme non dégénérée à plus de 5 variables représente 0 et on donne des conditions nécessaires et suffisantes dans les autres cas.

Théorème 4.1.2. *La forme q représente 0 si et seulement si l'une des conditions suivantes est vérifiée :*

i) $n = 2$ *et* $d(q) = -1 \pmod{k^{\times 2}}$ *;*
ii) $n = 3$ *et* $\left(\dfrac{-1, -d(q)}{p}\right) = \varepsilon(q)$ *;*
iii) $n = 4$ *et, soit* $d(q) \neq 1 \pmod{k^{\times 2}}$*, soit* $d(q) = 1 \pmod{k^{\times 2}}$ *et* $\varepsilon(q) = \left(\dfrac{-1, -1}{p}\right)$ *;*
iv) $n \geq 5$.

Avant de procéder à la démonstration, on énonce un corollaire fondamental :

Corollaire 4.1.1. Soit $a \in k^\times/k^{\times 2}$. Pour que q représente a, il faut et il suffit que :

i) $n = 1$ et $a = d(q) \pmod{k^{\times 2}}$;
ii) $n = 2$ et $\left(\dfrac{a, -d(q)}{p}\right) = \varepsilon(q)$;
iii) $n = 3$ et, soit $a \neq -d(q) \pmod{k^{\times 2}}$, soit $a = -d(q) \pmod{k^{\times 2}}$ et $\left(\dfrac{-1, -d(q)}{p}\right) = \varepsilon(q)$;
iv) $n \geq 4$.

Démonstration (du corollaire) : Soit $a \in k^\times/k^{\times 2}$, et soit $q_a = q - az^2$. D'après le corollaire 1.3.1, la forme q représente a si et seulement si q_a représente 0. Or, $d(q_a) = -ad(q)$ et $\varepsilon(q_a) = \varepsilon(q) \prod_{1 \leq i \leq n} \left(\dfrac{-a, a_i}{p}\right) = \varepsilon(q) \left(\dfrac{-a, d(q)}{p}\right)$. Une fois cette observation faite, il suffit d'appliquer le théorème à q_a.
i) Si $n = 1$, alors q_a est une forme à deux variables et elle représente 0 si et seulement si $d(q_a) = -1 \pmod{k^{\times 2}}$, c'est-à-dire $-ad(q) = -1 \pmod{k^{\times 2}}$, ou encore $d(q) = a \pmod{k^{\times 2}}$.
ii) Si $n = 2$, alors q_a est une forme à trois variables et la condition $\left(\dfrac{-1, -d(q_a)}{p}\right) = \varepsilon(q_a)$ est équivalente à $\left(\dfrac{-1, ad(q)}{p}\right) = \varepsilon(q) \left(\dfrac{-a, d(q)}{p}\right)$. En développant les symboles de Hilbert et en simplifiant, cette dernière est équivalente à $\left(\dfrac{a, -d(q)}{p}\right) = \varepsilon(q)$.
iii) Si $n = 3$, alors q_a est une forme à 4 variables et soit $d(q_a) \neq 1, \pmod{k^\times/k^{\times 2}}$, ceci est équivalent à $a \neq -d(q) \pmod{k^{\times 2}}$, soit $a = -d(q) \pmod{k^{\times 2}}$ et $\varepsilon(q) \left(\dfrac{-a, d(q)}{p}\right) = \varepsilon(q_a) = \left(\dfrac{-1, -1}{p}\right)$, ce qui équivaut à $a = -d(q) \pmod{k^{\times 2}}$ et $\varepsilon(q) = \left(\dfrac{-1, d(q)}{p}\right)\left(\dfrac{a, d(q)}{p}\right) = \left(\dfrac{-1, d(q)}{p}\right)$. En effet, il existe $x \in k^\times$ tel que $a = -d(q)x^2$, donc d'après la proposition 3.1.1, $\left(\dfrac{a, d(q)}{p}\right) = \left(\dfrac{-d(q)x^2, d(q)}{p}\right) = 1$.
iv) Enfin, si $n \geq 4$, la forme q_a a au moins 5 variables, donc elle représente 0. □

Passons maintenant à la démonstration du théorème :

Démonstration (du théorème) : Nous traitons les cas $n = 2, 3, 4$ et $n \geq 5$ séparément. À

chaque fois, l'existence d'une base orthogonale et la non dégénérescence nous permettent de supposer q équivalente à $a_1x_1^2 + \cdots + a_nx_n^2$.
i) Si $n = 2$, alors $a_2 \neq 0$ et puisque représenter 0 ne dépend pas de la base considérée, la forme q représente 0 si et seulement si $-a_1/a_2$ est un carré dans $k^\times$. Or, $-a_1/a_2 = -(a_1/a_2)\,a_2^2 = -d(q) \pmod{k^{\times 2}}$. On doit donc avoir $-d(q) = 1 \pmod{k^{\times 2}}$, c'est-à-dire $d(q) = -1 \pmod{k^{\times 2}}$.
ii) Si $n = 3$, alors $a_3 \neq 0$ et la forme q représente 0 si et seulement si $-a_3q$ représente 0, ou encore, si et seulement si $-a_3a_1x_1^2 - a_3a_2x_2^2 - a_3^2x_3^2 \sim -a_3a_1x_1^2 - a_3a_2x_2^2 - x_3^2$ représente 0. Par définition du symbole de Hilbert, ceci est équivalent à :

$$\left(\frac{-a_3a_1, -a_3a_2}{p}\right) = 1.$$

On développe en utilisant la bilinéarité et la symétrie du symbole de Hilbert :

$$\left(\frac{-a_3a_1, -a_3a_2}{p}\right) = \left(\frac{-1, -1}{p}\right)\left(\frac{-1, a_3}{p}\right)\left(\frac{-1, a_2}{p}\right)\left(\frac{a_3, -1}{p}\right)\left(\frac{a_3, a_3}{p}\right)\left(\frac{a_3, a_2}{p}\right)$$
$$\left(\frac{a_1, -1}{p}\right)\left(\frac{a_1, a_3}{p}\right)\left(\frac{a_1, a_2}{p}\right)$$
$$= \left(\frac{-1, -1}{p}\right)\left(\frac{-1, a_1}{p}\right)\left(\frac{-1, a_2}{p}\right)\left(\frac{a_3, a_3}{p}\right)\left(\frac{a_1, a_2}{p}\right)\left(\frac{a_1, a_3}{p}\right)\left(\frac{a_2, a_3}{p}\right)$$

D'après la proposition 3.1.1, $\left(\frac{a_3, -a_3}{p}\right) = 1$ donc $\left(\frac{a_3, a_3}{p}\right) = \left(\frac{-1, a_3}{p}\right)$, d'où :

$$1 = \left(\frac{-a_3a_1, -a_3a_2}{p}\right) = \left(\frac{-1, -1}{p}\right)\left(\frac{-1, a_1a_2a_3}{p}\right)\left(\frac{a_1, a_2}{p}\right)\left(\frac{a_1, a_3}{p}\right)\left(\frac{a_2, a_3}{p}\right),$$

ce qu'on réécrit $\left(\frac{-1, -d(q)}{p}\right)\varepsilon(q) = 1$, donc $\left(\frac{-1, -d(q)}{p}\right) = \varepsilon(q)$.

iii) Si $n = 4$, on écrit $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 = a_1x_1^2 + a_2x_2^2 - (-a_3x_3^2 - a_4x_4^2)$, d'après le corollaire 1.3.2, q représente 0 si et seulement si il existe $x \in k^\times/k^{\times 2}$ qui est représenté par les deux formes $q_1(x_1, x_2) = a_1x_1^2 + a_2x_2^2$ et $q_2(x_3, x_4) = -a_3x_3^2 - a_4x_4^2$. Ces formes sont en deux variables, on peut donc utiliser le cas *ii*) du corollaire (qui repose sur le cas *ii*) du théorème, qu'on vient de prouver) ; $x \in k^\times/k^{\times 2}$ est caractérisé par :

$$\left(\frac{x, -d(q_1)}{p}\right) = \varepsilon(q_1) \quad \text{et} \quad \left(\frac{x, -d(q_2)}{p}\right) = \varepsilon(q_2),$$

c'est-à-dire :

$$\left(\frac{x, -a_1a_2}{p}\right) = \left(\frac{a_1, a_2}{p}\right) \quad \text{et} \quad \left(\frac{x, -a_3a_4}{p}\right) = \left(\frac{-a_3, -a_4}{p}\right)$$

Soient A l'ensemble des éléments de $k^\times/k^{\times 2}$ vérifiant la première condition, et B l'ensemble de ceux qui vérifient la seconde. On raisonne par contraposition. Pour que q ne représente pas 0, il faut et il suffit que $A \cap B = \emptyset$, or A et B sont non vides puisque $a_1 \in A$ et $-a_3 \in B$; on peut donc appliquer le lemme 4.1.1. La relation $A \cap B = \emptyset$ équivaut à :

$$a_1a_2 = a_3a_4 \quad \text{et} \quad \left(\frac{a_1, a_2}{p}\right) = -\left(\frac{-a_3, -a_4}{p}\right).$$

La première condition donne $d(q) = a_1a_2a_3a_4 = (a_1a_2)^2 = 1 \pmod{k^{\times 2}}$. Si elle est vérifiée, on a :

$$\begin{aligned}
\varepsilon(q) &= \left(\frac{a_1, a_2}{p}\right)\left(\frac{a_1, a_3}{p}\right)\left(\frac{a_1, a_4}{p}\right)\left(\frac{a_2, a_3}{p}\right)\left(\frac{a_2, a_4}{p}\right)\left(\frac{a_3, a_4}{p}\right) \\
&= \left(\frac{a_1, a_2}{p}\right)\left(\frac{a_1, a_3a_4}{p}\right)\left(\frac{a_2, a_3a_4}{p}\right)\left(\frac{a_3, a_4}{p}\right) \\
&= \left(\frac{a_1, a_2}{p}\right)\left(\frac{a_1a_2, a_3a_4}{p}\right)\left(\frac{a_3, a_4}{p}\right) \\
&= \left(\frac{a_1, a_2}{p}\right)\left(\frac{a_3a_4, a_3a_4}{p}\right)\left(\frac{a_3, a_4}{p}\right) \\
&= \left(\frac{a_1, a_2}{p}\right)\left(\frac{-1, a_3a_4}{p}\right)\left(\frac{a_3, a_4}{p}\right) \\
&= \left(\frac{a_1, a_2}{p}\right)\left(\frac{-1, a_3}{p}\right)\left(\frac{-a_3, a_4}{p}\right) \\
&= \left(\frac{a_1, a_2}{p}\right)\left(\frac{-1, -1}{p}\right)\left(\frac{-1, -a_3}{p}\right)\left(\frac{-a_3, a_4}{p}\right) \\
&= \left(\frac{a_1, a_2}{p}\right)\left(\frac{-a_3, -a_4}{p}\right)\left(\frac{-1, -1}{p}\right)
\end{aligned}$$

Entre les lignes (4) et (5) on a utilisé le fait que le symbole de Hilbert vérifie $\left(\frac{x, x}{p}\right) = \left(\frac{-1, x}{p}\right)$.

Par hypothèse, $\left(\frac{a_1, a_2}{p}\right) = -\left(\frac{-a_3, -a_4}{p}\right)$ donc la condition s'écrit finalement :

$$\varepsilon(q) = -\left(\frac{-1, -1}{p}\right).$$

Ce qui achève la preuve de ce cas.
iv) Pour $n \geq 5$, nous observons qu'il suffit de traiter le cas $n = 5$. En effet, si q est une forme à $n \geq 5$, alors $\tilde{q}(x_1, \ldots, x_5) := q(x_1, \ldots, x_5, 1, \ldots, 1)$ est une forme à 5 variables et tout vecteur isotrope de $\tilde{q}$ donne un vecteur isotrope de q. D'après *ii*) du corollaire, une forme q' de rang 2 représente un élément $x \in k^\times/k^{\times 2}$ si et seulement si $\left(\frac{x, -d(q')}{p}\right) = \varepsilon(q')$. Avec les notations du lemme 4.1.1, on observe que ceci est équivalent à $x \in H^{\varepsilon(q')}_{-d(q')}$.On applique le lemme 4.1.1 : si $-d(q) \neq 1$, cet ensemble a 2^{r-1} éléments, sinon $-d(q) = 1$ et $H^{\varepsilon(q')}_{-d(q')}$ est non vide (la forme représente toujours au moins un élément) donc il a 2^r éléments. Dans tous les cas, $H^{\varepsilon(q')}_{-d(q')}$ a au moins 2^{r-1} éléments donc q représente au moins 2^{r-1} éléments. C'est *a fortiori* vrai pour les formes de rangs supérieurs, en particulier q représente au moins un élément $a \in k^\times/k^{\times 2}$ différent de $d(q)$. D'après le corollaire 1.3.1, q est équivalente à $ax^2 + q_1$, où q_1 est une forme de rang 4. Puisque $d(q) = ad(q_1)$, on a $d(q_1) = d(q)/a \neq 1 \pmod{k^{\times 2}}$. D'après *iii*), la forme q_1 représente 0, donc q aussi. Ce qui achève la démonstration du théorème. $\square$

4.2 Classification sur $\mathbb{Q}_p$

On peut désormais énoncer le résultat de classification des formes quadratiques sur $\mathbb{Q}_p$:

Théorème 4.2.1. *Soient q et q' deux formes quadratiques sur $\mathbb{Q}_p$, alors on a :*

$$q \sim q' \iff (rg(q) = rg(q'),\ d(q) = d(q') \text{ et } \varepsilon(q) = \varepsilon(q')).$$

Démonstration : Le sens direct est immédiat. Réciproquement, on procède par récurrence sur $n = \mathrm{rg}(q)$ $(= \mathrm{rg}(q'))$. Le résultat est vrai pour $n = 0$. Ensuite, on sait d'après le corollaire 4.1.1 que q et q' représentent les mêmes éléments de $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$. Soit donc a un tel élément. On écrit $q \sim aZ^2 + q_1$ et $q' \sim aZ^2 + q_1'$ où $\mathrm{rg}(q_1) = \mathrm{rg}(q_1') = n-1$. On a alors $d(q_1) = ad(q) = ad(q') = d(q_1')$ et $\varepsilon(q_1) = \varepsilon(q)\left(\dfrac{a, d(q_1)}{p}\right) = \varepsilon(q')\left(\dfrac{a, d(q_1')}{p}\right) = \varepsilon(q_1')$. D'après l'hypothèse de récurrence, on a $q_1 \sim q_1'$, d'où $q \sim q'$. □

Corollaire 4.2.1. À équivalence près, il existe une unique forme q sur $\mathbb{Q}_p$ de rang 4 qui ne représente pas 0. On a $q \sim Z^2 - aX^2 - bY^2 + abT^2$ où $\left(\dfrac{a, b}{p}\right) = -1$.

Démonstration : D'après le théorème 4.1.2, on a nécessairement $d(q) = 1$ et $\varepsilon(q) = -\left(\dfrac{-1, -1}{p}\right)$, ce qui est vérifié par $q \sim Z^2 - aX^2 - bY^2 + abT^2$. □

Proposition 4.2.1. Soit $n \geq 1$, $d \in \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$, et $\varepsilon \in \{\pm 1\}$, alors il existe q telle que $rg(q) = n$, $d(q) = d$, $\varepsilon(q) = \varepsilon$ si et seulement si :
i) $n = 1$ et $\varepsilon = 1$
ii) $n = 2$ et $d \neq -1 \pmod{\mathbb{Q}_p^{\times 2}}$
iii) $n = 2$ et $\varepsilon = 1$
iv) $n \geq 3$

Démonstration : i) Le cas où $n = 1$ est immédiat.
ii) Cas où $n = 2$: on écrit $q \sim aX^2 + bY^2$. Si on avait $d(q) = -1$ alors $\varepsilon(q) = \left(\dfrac{a, b}{p}\right) = \left(\dfrac{a, -ab}{p}\right) = 1$. Réciproquement, dans le cas où $d = -1$ et $\varepsilon = 1$, on prend $q = X^2 - Y^2$. Si $d \neq -1$, il existe $a \in k^\times$ tel que $\left(\dfrac{a, -d}{p}\right) = \varepsilon$, et $q = aX^2 + adY^2$ convient.
iii) Cas où $n = 3$: soit $a \in \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$ distinct de $-d$. On sait qu'il existe q' telle que $rg(q') = 2$, $d(q') = ad$ et $\varepsilon(q') = \varepsilon\left(\dfrac{a, -d}{p}\right)$. Alors $q = aZ^2 + q'$ convient. (On a en particulier $\varepsilon(q) = \left(\dfrac{a, d(q')}{p}\right)\varepsilon(q') = \left(\dfrac{a, ad}{p}\right)\varepsilon\left(\dfrac{a, -d}{p}\right) = \varepsilon$.
iv) Cas où $n \geq 4$: on se ramène au cas $n = 3$ en prenant q de la forme $q'(X_1, X_2, X_3) + X_4^2 + \cdots + X_n^2$, où $\mathrm{rg}(q') = 3$, $d(q') = d$ et $\varepsilon(q') = \varepsilon$).

□

Corollaire 4.2.2. Notons $m_{n,p}$ le nombre de classes d'équivalence de formes quadratiques sur $\mathbb{Q}_p$.
Si $p \neq 2$, on a : $m_{1,p} = 4$, $m_{2,p} = 7$, et $m_{n,p} = 8$ si $n \geq 3$.
Si $p = 2$, on a : $m_{1,2} = 8$, $m_{2,2} = 15$, et $m_{n,2} = 16$ si $n \geq 3$.

Démonstration : Si $p \neq 2$ (resp. si $p = 2$), on a $|\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}| = 4$ (resp. $= 8$) donc d peut prendre 4 valeurs (resp. 8 valeurs), et $\varepsilon \in \{\pm 1\}$ peut prendre deux valeurs. □

4.3 Théorème de Hasse-Minkowski

On note toujours $\mathcal{V} = \{\text{nombres premiers}\} \cup \{\infty\}$, et $\mathbb{Q}_\infty = \mathbb{R}$.

Dans toute cette section, $q \sim a_1X_1^2 + \cdots + a_nX_n^2$ désigne une forme quadratique de rang n à coefficients $a_i \in \mathbb{Q}$. On définit les invariants suivants :

Le discriminant $d(q) = a_1 \cdots a_n \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$.
Soit $v \in \mathcal{V}$, l'injection $\mathbb{Q} \to \mathbb{Q}_v$ fournit une forme quadratique q_v à coefficients dans $\mathbb{Q}_v$. On note $d_v(q) = d(q_v)$ (et $d_v(q)$ est l'image de $d(q)$ par $\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \to \mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2}$) et $\varepsilon_v(q) = \varepsilon(q_v)$. On a les relations suivantes :

$$\varepsilon_v(q) = \prod_{1 \leq i < j \leq n} \left(\frac{a_i, a_j}{v}\right) \quad \text{et} \quad \prod_{v \in \mathcal{V}} \varepsilon_v(q) = 1.$$

On définit la signature (r, s) de f comme étant la signature de f_∞.

Le théorème fondamental suivant, prouvé par Helmut Hasse en 1923, illustre le principe *local-global* : pour étudier une forme quadratique sur $\mathbb{Q}$ il est suffisant de l'étudier sur $\mathbb{R}$ et sur $\mathbb{Q}_p$ pour p premier.

Théorème 4.3.1 (Hasse-Minkowski)**.** *On a l'équivalence suivante :*

$$q \textit{ représente } 0 \iff \textit{pour tout } v \in \mathcal{V},\ q_v \textit{ représente } 0.$$

Démonstration : Le sens direct est immédiat. Pour la réciproque, écrivons $q = a_1X_1^2 + \cdots + a_nX_n^2$ où $a_i \in \mathbb{Q}^\times$. On peut supposer que $a_1 = 1$ (quitte à remplacer q par $a_1^{-1}q$).

- Cas où $n = 2$: La forme q_∞ représente 0, donc on peut écrire $q = X_1^2 - aX_n^2$, où $a > 0$. Écrivons $a = \prod_p p^{v_p(a)}$. Comme q_p représente 0, $a \in \mathbb{Q}_p^{\times 2}$ et $v_p(a)$ est pair pour tout premier p, ce qui implique que $a \in \mathbb{Q}^2$ et q représente 0.
- La démonstration du cas $n = 3$ est due à Legendre. On a $q = Z^2 - aX^2 - bY^2$ où l'on peut supposer a et b non nuls et sans facteurs carrés (quitte à multiplier par des carrés) ainsi que $|a| \leq |b|$.
On procède par récurrence sur $m = |a| + |b|$.
Si $m = 2$, on a $q = Z^2 \pm X^2 \pm Y^2$. Comme q représente 0, on peut exclure $Z^2 + X^2 + Y^2$, et dans les autres cas q représente 0.
Si $m > 2$ (*i.e.* $b \geq 2$), écrivons $b = \pm p_1 \cdots p_k$, où les p_i sont des nombres premiers

distincts. Fixons un facteur premier p de b et montrons que a est un carré modulo p. C'est le cas si $a = 0 \pmod p$ (On a vu que dans ce cas $\left(\dfrac{a}{p}\right) = 0$). Ensuite, si $a \neq 0 \pmod p$, alors $a \in \mathbb{U}$. Comme q représente 0 sur $\mathbb{Q}_p$, il existe $(x, y, z) \in (\mathbb{Q}_p)^3 \backslash \{(0,0,0)\}$ tel que $z^2 - ax^2 - by^2 = 0$. D'après la proposition 2.3.2, on peut supposer $(x, y, z) \in (\mathbb{Z}_p)^3 \backslash \{(0,0,0)\}$ primitif. On a $z^2 - ax^2 = 0 \pmod p$. Supposons par l'absurde que $x = 0 \pmod p$, alors $z^2 = 0 \pmod p$ donc $z = 0 \pmod p$. Cela entraîne $by^2 = 0 \pmod{p^2}$, avec $v_p(b) = 1$, donc $y = 0 \pmod p$, ce qui contredit le fait que (x, y, z) est primitif. Ainsi $x \neq 0 \pmod p$, donc $x \in \mathbb{U}$ et $a = (zx^{-1})^2 \pmod p$ est un carré. D'après le théorème chinois, $\mathbb{Z}/b\mathbb{Z} \simeq \prod_{1 \leq i \leq k} \mathbb{Z}/p_i\mathbb{Z}$, donc a est un carré modulo b. Soient alors $t, b' \in \mathbb{Z}$ tels que $t^2 - a = bb'$. On peut choisir $|t| < \frac{|b|}{2}$ (prendre un représentant de $t \pmod b$ dans $]-b/2; b/2[$). Comme bb' est une norme dans $k_a := k(\sqrt{a})/k$ (où $k = \mathbb{Q}$ ou $\mathbb{Q}_v$), le lemme 3.1.2 montre que la forme q représente 0 sur k si et seulement si $b \in N_{k_a^\times}$, si et seulement si $b' \in N_{k_a^\times}$, si et seulement si $q' = z^2 - ax^2 - b'y^2$ représente 0 sur k. Or $|b'| = |\frac{t^2-a}{b}| \leq \frac{|b|}{4} + 1 < |b|$ (puisque $|b| > 2$). On écrit $b' = b''u^2$ où b'' est sans facteurs carrés, alors $|b''| < |b|$, et par hypothèse de récurrence, $q'' = Z^2 - aX^2 - b''Y^2$ représente 0 dans $\mathbb{Q}$, donc $q \sim q''$ aussi.

- Cas où $n = 4$: Écrivons $q \sim f \dot{-} g \sim (aX_1^2 + bX_2^2) - (cX_3^2 + dX_4^2)$. Si $v \in \mathcal{V}$, q_v représente 0 donc d'après le corollaire 1.3.2, il existe $x_v \in \mathbb{Q}_v^\times$ représenté par f et g. D'après le corollaire 4.1.1, on a :

$$\left(\frac{x_v, -d(f)}{v}\right) = \varepsilon(f), \ \ i.e. \left(\frac{x_v, -ab}{v}\right) = \left(\frac{a, b}{v}\right),$$

et de même,

$$\left(\frac{x_v, -cd}{v}\right) = \left(\frac{c, d}{v}\right).$$

Comme $\prod_{v \in \mathcal{V}} \left(\dfrac{a, b}{v}\right) = \prod_{v \in \mathcal{V}} \left(\dfrac{c, d}{v}\right) = 1$, on sait d'après le théorème 3.2.2 qu'il existe $x \in \mathbb{Q}^\times$ tel que pour tout $v \in \mathcal{V}$:

$$\left(\frac{x, -ab}{v}\right) = \left(\frac{a, b}{v}\right) \text{ et } \left(\frac{x, -cd}{v}\right) = \left(\frac{c, d}{v}\right).$$

Par conséquent $f - xZ^2$ représente 0 dans $\mathbb{Q}_v$ pour tout $v \in \mathcal{V}$ donc elle représente 0 sur $\mathbb{Q}$ (cas où $n = 3$), et f représente x. De même on montre que g représente x, d'où q représente 0.

- Cas où $n \geq 5$: Par récurrence sur n. On écrit $q \sim f \dot{-} g$ où $f = a_1X_1^2 + a_2X_2^2$ et $g = -(a_3X_3^2 + \cdots + a_nX_n^2)$. Soit $S \subset \mathcal{V}$ défini par :

$$S = \{p \text{ premier} \mid \exists\, i \geq 3 : v_p(a_i) \neq 0\} \cup \{2, \infty\}.$$

qui est un ensemble fini. Comme q_v représente 0, il existe $b_v \in \mathbb{Q}_v^\times$ représenté à la fois par f et g dans $\mathbb{Q}_v^\times$. Écrivons $b_v = f(x_{1,v}, x_{2,v}) = g(x_{3,v}, \ldots, x_{n,v})$. D'après le corollaire 2.4.5, on sait que $\mathbb{Q}_v^{\times 2}$ est ouvert dans $\mathbb{Q}_v^\times$, et d'après le lemme 3.2.1, on sait que $\mathbb{Q}$ est dense dans $\prod_{v \in S} \mathbb{Q}_v$. Comme f est continue, $f^{-1}(b_v\mathbb{Q}_v^{\times 2})$ est un ouvert non vide de $\mathbb{Q}_v \times \mathbb{Q}_v$ (c'est aussi un voisinage de $(x_{1,v}, x_{2,v})$), donc il existe $(x_1, x_2) \in \mathbb{Q} \times \mathbb{Q}$ tel que $b := f(x_1, x_2) \in \mathbb{Q}$ vérifie : $\frac{b}{b_v} \in \mathbb{Q}_v^{\times 2}$. Comme g représente b_v sur $\mathbb{Q}_v$, elle représente aussi b, donc $g_1 = bZ^2 \dot{-} g$ représente 0 dans $\mathbb{Q}_v$ pour $v \in S$.

Si $v \notin S$, on a $v_v(a_i) = 0$ pour tout $i \geq 3$, donc $v_v(d_v(g)) = 0$ *i.e.* $d_v(g)$ est une unité v-adique. On a $\varepsilon_v(g) = \prod_{3\leq i<j\leq n} \left(\frac{-a_i, -a_j}{v}\right) = 1$ car $v \neq 2$. De plus $\mathrm{rg}(g) \geq 3$, donc g représente 0 dans $\mathbb{Q}_v$ d'après le corollaire 1.1.2, puis g_1 représente 0 dans $\mathbb{Q}_v$. Ensuite $\mathrm{rg}(g_1) = n - 1$, donc par hypothèse de récurrence g_1 représente 0 sur $\mathbb{Q}$, donc g représente b sur $\mathbb{Q}$, donc q aussi.

$\square$

Corollaire 4.3.1. Soit $a \in \mathbb{Q}^\times$. On a l'équivalence :

$$q \text{ représente } a \text{ dans } \mathbb{Q} \iff \text{pour tout } v \in \mathcal{V},\ q \text{ représente } a \text{ dans } \mathbb{Q}_v.$$

Démonstration : On applique le théorème précédent à $aZ^2 - q$. $\square$

Corollaire 4.3.2 (Meyer)**.** Supposons $rg(q) \geq 5$, alors q représente 0 si et seulement si elle est *indéfinie* (*i.e.* q représente 0 sur $\mathbb{R}$).

Démonstration : Cela résulte du théorème 4.1.2, puisque q représente 0 dans $\mathbb{Q}_v$ pour tout $v \in \mathcal{V}$. $\square$

Corollaire 4.3.3. Supposons $\mathrm{rg}(q) = 3$ (resp. $\mathrm{rg}(q) = 4$ et $d(q) = 1$). Si q représente 0 dans tous les $\mathbb{Q}_v$ sauf au plus un, alors q représente 0.

Démonstration :

- Pour $n = 3$, toujours d'après le théorème 4.1.2, on sait que :
$$q \text{ représente } 0 \text{ dans } \mathbb{Q}_v \iff \left(\frac{-1, -d(q)}{v}\right) = \varepsilon_v(q) \quad (E_v).$$
Or $\prod\limits_{v\in\mathcal{V}} \varepsilon_v(q) = 1$ et $\prod\limits_{v\in\mathcal{V}} \left(\frac{-1, -d(q)}{v}\right) = 1$ en vertu du théorème 3.2.1. Donc si l'égalité (E_v) est vérifiée pour tout $v \in \mathcal{V}$ sauf au plus un, elle est vraie pour tout v, et q représente 0.
- Pour $n = 4$ et $d(q) = 1$, on remplace (par application du théorème 4.3.1) l'égalité (E_v) par $\left(\frac{-1, -1}{v}\right) = \varepsilon_v(q)$.

$\square$

4.4 Classification sur $\mathbb{Q}$

Théorème 4.4.1. *Soient q et q' deux formes quadratiques sur $\mathbb{Q}$. Elles sont équivalentes si et seulement elles le sont sur $\mathbb{Q}_v$ pour tout $v \in \mathcal{V}$.*

Démonstration : Le sens direct est immédiat. Pour la réciproque, on procède par récurrence sur $n = \mathrm{rg}(q) = \mathrm{rg}(q')$. Le résultat est vrai pour $n = 0$. Si $n > 0$, soit $a \in \mathbb{Q}^\times$ représenté par q. D'après le théorème 4.3.1 q' représente a. Écrivons $q \sim aZ^2 + q_0$ et $q' \sim aZ^2 + q_0'$. D'après le théorème de simplification de Witt, on a $q_0 \sim q_0'$ sur $\mathbb{Q}_v$, et ce pour tout $v \in \mathcal{V}$. Par hypothèse de récurrence, on a $q_0 \sim q_0'$ sur $\mathbb{Q}$, et donc $q \sim q'$ sur $\mathbb{Q}$. $\square$

Corollaire 4.4.1. Soient (r,s) et (r',s') les signatures de q et q'. On a l'équivalence :

$$q \sim q' \iff \begin{cases} d(q) &= d(q') \\ (r,s) &= (r',s') \\ \varepsilon_v(q) &= \varepsilon_v(q') \quad \text{pour tout } v \in V \end{cases}$$

Démonstration : Ce sont les conditions pour que $q \sim q'$ sur $\mathbb{Q}_v$. □

Remarque : Notons $d = d(q)$, $\varepsilon_v = \varepsilon_v(q)$, et (r,s) les invariants de q. Ils vérifient les relations suivantes :

- $\varepsilon_v = 1$ pour presque tout $v \in \mathcal{V}$ et $\displaystyle\prod_{v\in\mathcal{V}} \varepsilon_v = 1$.
- $\varepsilon_v = 1$ si $n = 1$, ou si $n = 2$ et l'image d_v de d dans $\mathbb{Q}_v/\mathbb{Q}_v^{\times 2}$ vaut -1.
- $r, s \geq 0$ et $r + s = n$.
- $d_\infty = (-1)^s$.
- $\varepsilon_\infty = (-1)^{s(s-1)/2}$.

Proposition 4.4.1. Soit $d, (\varepsilon_v)_{v\in\mathcal{V}}$ et (r,s) vérifiant ces relations, alors il existe une forme quadratique de rang n sur $\mathbb{Q}$ ayant ces invariants.

Démonstration :

- Le cas $n = 1$ est immédiat.
- Si $n = 2$, soit $v \in \mathcal{V}$, on sait qu'il existe $x_v \in \mathbb{Q}_v^\times$ tel que $\left(\dfrac{x_v, -d}{v}\right) = \varepsilon_v$ (par non-dégénérescence du symbole de Hilbert). D'après le théorème 3.2.2, la première condition implique qu'il existe $x \in \mathbb{Q}^\times$ tel que $\left(\dfrac{x, -d}{v}\right) = \varepsilon_v$, et ce pour tout $v \in \mathcal{V}$. Il suffit de considérer $q = xX^2 + xdY^2$.
- Cas où $n = 3$. Soit $S = \left\{ v \in \mathcal{V} \mid \left(\dfrac{-d, -1}{v}\right) = -\varepsilon_v \right\}$. C'est un ensemble fini, et si $v \in S$, choisissons $c_v \in \mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2}$ distinct de $-d_v$. D'après le théorème d'approximation 3.2.1, il existe $c \in \mathbb{Q}^\times$ d'image c_v dans $\mathbb{Q}_v^\times/\mathbb{Q}_v^{\times 2}$. On sait qu'il existe q telle que $\mathrm{rg}(q) = 2$, $d(q) = cd$, $\varepsilon_v(q) = \left(\dfrac{c, -d}{v}\right)\varepsilon_v$ pour tout $v \in \mathcal{V}$. Il suffit alors de considérer $q' = q \dot{+} cZ^2$.
  Notons que pour $1 \leq n \leq 3$, la signature est entièrement déterminée par d_∞ et ε_∞.
- Cas où $n \geq 4$. On procède par récurrence sur n. Supposons que $r \geq 1$. Par hypothèse de récurrence, il existe q telle que $\mathrm{rg}(q) = n-1$, $d(q) = d$, $\varepsilon_v(q) = \varepsilon_v$ pour tout v, et q est de signature $(r-1, s)$. On prend alors $q' = X^2 + q$. D'autre part si $r = 0$ (et donc $s = n$), soit q telle que $\mathrm{rg}(q) = n-1$, $d(q) = -d$, $\varepsilon_v(q) = \varepsilon_v \left(\dfrac{-1, -d}{v}\right)$ pour tout v, et q est de signature $(0, n-1)$. On prend alors $q' = -X^2 + q$.

□

Appendice

On montre dans cette section qu'un groupe topologique localement compact est complet.

Définition : Soit $(G, \cdot)$ un groupe. On dit que G est un groupe topologique s'il est muni d'une topologie telle que $(x, y) \mapsto xy^{-1}$ est continue.

Exemple : $(\mathbb{R}, +)$, $(\mathbb{Z}_p, +)$, $(\mathbb{Z}_p^\times, \times)$, $(\mathbb{Q}_p, +)$, $(\mathbb{Q}_p^\times, \times)$ sont des groupes topologiques. On vérifie en particulier que $(x, y) \mapsto x - y$ et $(x, y) \mapsto xy^{-1}$ sont continues.

Lemme : Soit G un groupe topologique et H un sous-groupe de G. Alors :

(i) L'adhérence $\overline{H}$ de H est un sous-groupe de G.

(ii) G est séparé si et seulement si $\{e\}$ est fermé.

Démonstration : (i) Soit $\varphi : G \times G \to G$ l'application continue $\varphi(x, y) = xy^{-1}$. H étant un sous-groupe, on a $\varphi(H \times H) \subset H$. Alors : $\varphi(\overline{H} \times \overline{H}) = \varphi(\overline{H \times H}) \subset \overline{\varphi(H \times H)} \subset \overline{H}$, et $\overline{H}$ est un sous-groupe.
(ii) Un espace X est séparé si et seulement si la diagonale $\Delta = \{(x, x) \in X\}$ est fermée dans $X \times X$. Alors : G est séparé $\Leftrightarrow \Delta = \varphi^{-1}(e)$ est fermé dans $G \times G \Leftrightarrow \{e\}$ est fermé. □

Lemme : Soit G un groupe topologique et H un sous-groupe de G. Si H contient un voisinage de e (élément neutre), alors H est à la fois ouvert et fermé dans G.
Démonstration : Soit V un voisinage de $\{e\}$ dans G contenu dans H.
- H est ouvert : soit $h \in H$, alors hV est un voisinage de h contenu dans H (remarquons que l'application $x \mapsto hx$ est un homéomorphisme), ce qui montre que H est un voisinage de chacun de ses points.
- H est fermé : gH est ouvert pour tout $g \in G$ (puisque H est ouvert et que les translations sont des homéomorphismes), toute union de ces ensembles est ouverte. Comme $H = \left(\bigcup_{gH \neq H} gH \right)^c$, H est fermé. □

Théorème : Soit G un groupe topologique et H un sous-groupe localement fermé. Alors H est fermé.
Démonstration : Si H est localement fermé dans G, alors H est ouvert dans $\overline{H}$, qui est un sous-groupe topologique de G. D'après le lemme précédent, H est fermé dans $\overline{H}$ et $H = \overline{H}$.
□

Corollaire : Un groupe topologique métrisable localement compact est complet.

Démonstration : Soit $\hat{G}$ un complété de G. C'est aussi un groupe topologique. Comme G est localement compact, il est fermé dans son complété. □

Bibliographie

- M. Aigner, *Raisonnements divins*, Hermes Science, 2017.
- O. Brinon, *Cours de Master 1 : Modules, Espaces Quadratiques*, 2017.
- F. Gouvêa, *p-adic numbers, an introduction*, Springer, 1997.
- N. Koblitz, *p-adic Numbers, p-adic Analysis and Zeta-Functions*, Springer, 1984.
- F. Lemmermeyer, *Reciprocity Laws*, Springer, 2000.
- A. Robert, *A Course in p-adic Analysis*, Springer, 2000.
- J.P. Serre, *Cours d'arithmétique*, Presse Universitaire de France, 1970.