Mini-projet

Mathieux Tony

27 janvier 2016

Table des matières

Chapitre 1

Avant-propos.

Les équations diophantiennes, du nom du mathématicien grec Diophante (III^e siècle après J.C), sont des équations polynômiales en plusieurs variables, dont on cherche des solutions en nombres entiers ou rationnels. La résolution de ces équations est généralement difficile et utilise des outils variés tels que les nombres p-adiques, les anneaux d'entiers d'un corps de nombres ou encore la géométrie des nombres dans les réseaux de $\mathbb{R}^n$ par exemples. Dans ce projet nous utiliserons essentiellement les nombres p-adiques ainsi que des formes quadratiques et nous nous intéressons aux équations diophantiennes

$$P(X_1, \ldots, X_n) = 0 \tag{1.1}$$

où $P \in \mathbb{Q}[X_1, \ldots, X_n]$ est un polynôme homogène. On remarque que pour ce type d'équation il revient au même de chercher des solutions dans $\mathbb{Q}^n/\{(0, \ldots, 0)\}$ ou dans $\mathbb{Z}^n/\{(0, \ldots, 0)\}$. Nous considérerons essentiellement le cas où P est de degré 2, le point central du projet étant la démonstration, au chapitre 6, du théorème de Hasse-Minkowsi qui illustre un principe «local-global» ; la démonstration proposée est extraite du livre de Jean-Pierre Serre [1]. Les parties 3.1, 3.2 et 5.1 sont composées d'énoncés sans démonstration (essentiellement des rappels) dans le but de faciliter les références à des notions et résultats supposés connus concernant les nombres p-adiques et les formes quadratiques. Les compléments du chapitre 7 présentent notamment un cas particulier où P est de degré 3 ainsi qu'une étude des systèmes d'équations diophantiennes homogènes de degré 1.

Chapitre 2

Introduction.

2.1 Paramétrage rationnel.

Commençons par déterminer les triplets Pythagoriciens c'est-à-dire les triplets $(x, y, z) \in \mathbb{N}^3$ tels que $x^2 + y^2 = z^2$.

Proposition 1 *Pour que $(x, y, z) \in \mathbb{N}^3$ soit solution de l'équation*

$$x^2 + y^2 = z^2 \tag{2.1}$$

il faut et il suffit qu'il existe $u, v \in \mathbb{N}$ premiers entre eux et $d \in \mathbb{N}$ tels que (x, y, z) ou (y, x, z) soit égal à $(d(u^2 - v^2), 2duv, d(u^2 + v^2))$.

Démonstration :

La condition est suffisante car :

$$\begin{aligned}(d(u^2 - v^2))^2 + (2duv)^2 &= d^2u^4 - 2d^2u^2v^2 + d^2v^4 + 4d^4u^2v^2 \\ &= (du^2)^2 + 2du^2dv^2 + (dv^2)^2 \\ &= (d(u^2 + v^2))^2.\end{aligned}$$

Montrons qu'elle est nécessaire. Soit $(x, y, z) \in \mathbb{N}^3$ vérifiant (2.1). Écartons le cas $xyz = 0$ qui est bien de la forme indiquée (par exemple si $y = 0$ alors on prend $u = 1$, $v = 0$ et $d = x(= z)$). En divisant x, y, z par $\text{pgcd}(x, y, z)$ on obtient une autre solution, on peut donc supposer que $\text{pgcd}(x, y, z) = 1$, on obtient les autres solutions en multipliant x, y, z par $d \in \mathbb{N}$. Par (2.1), x, y, z sont premiers entre eux deux à deux, en particulier il est impossible que deux de ces nombres soient pairs. De plus x et y ne peuvent être impairs tous les deux car on aurait alors $x^2 \equiv 1 \pmod 4, y^2 \equiv 1 \pmod 4$ d'où $z^2 = x^2 + y^2 \equiv 2 \pmod 4$ et alors 2 diviserait z et on aurait $z^2 \equiv 0 \pmod 4$ ce qui est absurde car $0 \not\equiv 2 \pmod 4$. Quitte à échanger x et y on peut donc supposer x impair et y pair. Nous terminons alors la preuve par un raisonnement d'arithmétique, une méthode alternative sera exposée dans la remarque suivante.

On écrit alors $y^2 = z^2 - x^2 = (z - x)(z + x)$. Comme le pgcd de $2x$ et $2z$ est 2, et que $2x = (z + x) - (z - x)$, $2z = (z+x)+(z-x)$, le pgcd de $z+x$ et de $z-x$ est égal à 2. Posons alors $y = 2y', z+x = 2x', z-x = 2z'$, où $x', y', z' \in \mathbb{Z}$. On a alors $y'^2 = x'z'$, et comme x' et z' sont premiers entre eux, nécéssairement x' et z' sont des carrés : $x' = u^2$ et $z' = v^2$, $u, v \in \mathbb{Z}$. On a donc $z + x = 2u^2$, $z - x = 2v^2$ et $y^2 = 2u^2 2v^2$ d'où $x = u^2 - v^2$, $y = 2uv$ et $z = u^2 + v^2$. De plus u et v sont premiers entre eux sinon x, y, z auraient un facteur premier en commun, ce qui est exclu. ◪

Remarque 1 *Une autre façon de terminer la preuve précédente et d'utiliser un paramétrage rationnel du cercle unité. Posons* $X = \frac{x}{z}$ *et* $Y = \frac{y}{z}$. *Alors* $x^2 + y^2 = z^2$ *si et seulement si* $X^2 + Y^2 = 1$. *Nous cherchons donc des points à coordonnées rationnels sur le quart de cercle trigonométrique* $X = \frac{x}{z} > 0, Y = \frac{y}{z} > 0$. *Or ce quart de cercle admet le paramétrage, où* $t \in]0, 1[$,

$$X = \frac{1-t^2}{1+t^2},\ Y = \frac{2t}{1+t^2}.$$

Si $t \in \mathbb{Q}$ *alors* $X, Y \in \mathbb{Q}$. *Réciproquement, si* $X, Y \in \mathbb{Q}$ *alors* $t^2 = \frac{1-X}{1+X} \in \mathbb{Q}$ *et donc* $t = \frac{1+t^2}{2}Y \in \mathbb{Q}$. *Ainsi, pour connaitre les solutions premières de* (2.1) *il suffit de choisir* $t \in \mathbb{Q}$ *et alors* x, y, z *sont déterminés par le fait que* $X = \frac{x}{z}$ *et* $Y = \frac{y}{z}$, *les fractions étant écrite sous formes réduites (c'est-à-dire que les fractions ont été simplifiées puis ramenées au plus petit dénominateur commun) avec* x *impair. Soient alors* $v \in \mathbb{N}, u \in \mathbb{N}^*$ *premiers entre eux, et* $t = \frac{v}{u}$. *On a :*

$$X = \frac{1-t^2}{1+t^2} = \frac{u^2-v^2}{u^2+v^2},\ Y = \frac{2t}{1+t^2} = \frac{2uv}{u^2+v^2}.$$

Vérifions que $u^2 - v^2, 2uv, u^2 + v^2$ *sont premiers dans leur ensemble, ils seront alors égaux respectivement à* x, y, z *par unicité de la forme réduite de* X *et* Z. *Soit* p *un diviseur premiers de ces trois nombres. Alors* p *divise* $(u^2 + v^2) + (u^2 - v^2) = 2u^2$ *et* $(u^2 + v^2) - (u^2 - v^2) = 2v^2$. *Si* $p \neq 2$ *alors* p *divise* u *et* v, *ce qui est exclu car* $\text{pgcd}(u, v) = 1$. *Donc* $p = 2$, *et le fait que* 2 *divise* $u^2 + v^2$ *nécéssite que* u *et* v *soient de même parité. Mais comme* u *et* v *sont premiers entre eux, ils doivent donc être impairs :* $u = 2k + 1$, $v = 2m + 1$ *et alors* $u^2 - v^2 = 4k + 4k^2 - 4m - 4m^2$, $2uv = 2(1 + 2k + 2m + 4km)$, $u^2 + v^2 = 2 + 4k + 4k^2 + 4m + 4m^2$. *On peut simplifier par* 2. *On obtient des nombres premiers entre eux dans leur ensemble qui seront égaux à* x, y, z *par unicité de la forme réduite de* X *et* Y. *Mais ceci implique que* x *est pair ce qui est exclu. Le facteur* 2 *est à rejeter et les trois nombres considérés sont effectivement premiers entre eux dans leur ensemble, égaux à* x, y, z. *Ainsi pour toute solution* $(x, y, z) \in \mathbb{N}^3$ *avec* $\text{pgcd}(x, y, z) = 1$, x *impair et* y *pair on a* z *impair et il existe* $u, v \in \mathbb{N}$ *premiers entre eux tels que* $x = u^2 - v^2, y = 2uv$ *et* $z = u^2 + v^2$. ◪

La méthode employée pour résoudre (2.1) est applicable à d'autres équations du type (1.1). Il suffit d'avoir un paramétrage rationnel de l'hypersurface (H) d'équation $P(x_1, \ldots, x_{n-1}, 1) = 0$. Pour obtenir un tel paramétrage on peut procéder de la manière suivante : connaissant un point z de cette hypersurface à coordonnées rationnelles, si une droite de pente rationnelle passe par z et rencontre l'hypersurface en y alors y est à coordonnées rationnelles, et réciproquement si y est un autre point de (H) à coordonnées rationnelles alors la droite passant par y et z est de pente rationnelle. On est donc parfois ramener à trouver, si elle existe, une solution non nulle (puisqu'on veut $P(x_1, \ldots, x_{n-1}, 1) = 0$) de (1.1). Le théorème de Hasse-Minkowski indique une condition nécéssaire est suffisante pour qu'une équation (1.1) avec P homogène de degré 2 admette une solution non nulle.

Terminons cette partie par un exemple de degré 3.

Exemple :
Considérons l'équation

$$x^3 + y^3 = xyz. \tag{2.2}$$

Montrons que $(x, y, z) \in \mathbb{Z}^3$ est solution de cette équation si et seulement s'il existe $u, v \in \mathbb{Z}$ premiers entre eux et $d \in \mathbb{Z}$ tels que $(x, y, z) = (duv^2, du^2v, d(u^3+v^3))$. Soit (x, y, z) une solution de (2.2). Si $z = 0$ alors l'ensemble des solutions est $\{(x, -x, 0), x \in \mathbb{Z}\}$. Soit $d = \text{pgcd}(x, y, z)$. On remarque que $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d})$ et $(-x, -y, -z)$ sont

solutions de (2.2), donc on peut supposer $d = 1$ et $z > 0$, on obtiendra alors toutes les solutions en multipliant x, y, z par un entier relatif. Posons $X = \frac{x}{z}$ et $Y = \frac{y}{z}$. Alors le point de coordonnées (X, Y) est à coordonnées rationnelles sur la courbe $\mathcal{C}$ de $\mathbb{R}^2$ d'équation $X^3 + Y^3 = XY$ (Folium de Descartes). Réciproquement, tout point M à coordonnées rationnelles (X, Y) de $\mathcal{C}$ autre que l'origine fournie une solution du type indiqué en exprimant les rationnels $X = \frac{x}{z}$ et $Y = \frac{y}{z}$ comme fractions réduites puis ramenées au plus petit dénominateur commun. En recoupant $\mathcal{C}$ avec les droites d'équations $Y = tX$, $t \in \mathbb{Q}$ on obtient le paramétrage rationnel $X = \frac{t}{1+t^3}$, $Y = \frac{t^2}{1+t^3}$ des points autres que l'origine. Pour $t \in \mathbb{Q}$ on a $X \in \mathbb{Q}$ et $Y \in \mathbb{Q}$. Réciproquement si $X \in \mathbb{Q}^*$ et $Y \in \mathbb{Q}$ alors $t := \frac{Y}{X} \in \mathbb{Q}$ (on a $X \neq 0$ en-dehors de l'origine). Pour tout $t = \frac{u}{v} \in \mathbb{Q}$ avec $u \in \mathbb{Z}^*$, $v \in \mathbb{N}^*$ et $\text{pgcd}(u, v) = 1$, on obtient $x = uv^2, y = u^2v, z = u^3 + v^3$ premiers dans leur ensemble (on remarque que les solutions $(0, 0, z)$, $z \in \mathbb{Z}$ sont aussi de cette forme). Réciproquement, pour tout $u, v \in \mathbb{Z}$, $(uv^2, u^2v, u^3 + v^3)$ est bien solution de (2.2). ◪

2.2 Réduction

Considérons l'équation :

$$P(X_1, \ldots, X_n) = 0 \quad \text{où } P \in \mathbb{Z}[X_1, \ldots, X_n]. \tag{2.3}$$

Dans le but de déterminer si cette équation possède ou non une solution, on peut l'étudier sur un anneau $\mathbb{Z}/n\mathbb{Z}$ ou sur un corps $\mathbb{Q}_p$. Dans cette partie nous allons considérer la réduction modulo un entier.

Proposition 2 *Si l'équation* (2.3) *admet une solution entière alors elle admet une solution dans* $\mathbb{Z}/n\mathbb{Z}$ *pour tout entier* n.

Démonstration :
Cela résulte immédiatement du fait que la projection canonique $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupes.

Exemple :
On considère l'équation $15x^2 - 7y^2 = 9$. Alors on obtient $-2y^2 \equiv -1 \pmod 5$ soit $2y^2 \equiv 1 \pmod 5$. Puis l'inverse de 2 modulo 5 est 3 donc on obtient l'équation $y^2 = 3$ dans $\mathbb{Z}/5\mathbb{Z}$. Or l'ensemble des carrés de $\mathbb{Z}/5\mathbb{Z}$ est $\{0, 1, 4\}$ donc l'équation n'a pas de solution.

En revanche la réciproque de la proposition est fausse comme le montre l'exemple suivant.

Proposition 3 *L'équation* $(E) : (x^2 - 13)(x^2 - 17)(x^2 - 221) = 0$ *n'admet pas de solution dans* $\mathbb{Z}$ *mais elle en admet dans* $\mathbb{Z}/n\mathbb{Z}$ *pour tout* $n \in \mathbb{N}^*$.

Démonstration :
Cette équation n'a pas de solutions entières car $13, 17$ et 221 ne sont pas des carrés dans $\mathbb{Z}$.
Montrons que cette équation a au moins une solution dans $\mathbb{Z}/n\mathbb{Z}$ ($n \in \mathbb{N}^*$). Le cas $n = 1$ est trivial. Par le lemme chinois il suffit de montrer que (E) a une solution dans $\mathbb{Z}/p^i\mathbb{Z}$ pour tout nombre premier p et tout entier non nul i. Soit p un nombre premier. On commence par montrer que (E) admet une solution dans $\mathbb{Z}/p\mathbb{Z}$, Pour cela on montre que 13 ou 17 ou 221 est un carré modulo p. On remarque que $221 = 13 \times 17$ et par la multiplicativité du symbole de Legendre on a, pour $p \neq 13, 17$, $\left(\frac{13}{p}\right)\left(\frac{17}{p}\right) = \left(\frac{221}{p}\right)$, donc soit 13 ou 17 est un carré modulo p, soit ni 13 ni 17 ne sont des carrés modulo p mais dans ce cas 221 est un carré modulo p, de plus 13 est un carré modulo 17 et 17 est un carré modulo 13, donc dans tous les cas (E) admet une solution dans $\mathbb{Z}/p\mathbb{Z}$.
La fin de la preuve résulte du lemme suivant (17 est un carré modulo 2 et $17 \equiv 1 \pmod 8$).

Lemme 1 *Soit p un nombre premier et $a \in \mathbb{Z}^*$ un carré modulo p.*
Si $p \neq 2$ alors a est un carré modulo p^i pour tout $i \in \mathbb{N}^*$.
Si $p = 2$ et si $a \equiv 1 \pmod 8$ alors a est un carré modulo p^i pour tout $i \in \mathbb{N}^*$.

Démonstration :
On raisonne par récurrence sur $i \in \mathbb{N}^*$. On note $\mathcal{P}_i$ la proposition «a est un carré modulo p^i».
Par hypothèse $\mathcal{P}_1$ est vraie.
Soit $i \in \mathbb{N}^*$, supposons que $\mathcal{P}_i$ est vraie et montrons que $\mathcal{P}_{i+1}$ est vraie.
Supposons dans un premier temps $p \neq 2$. Comme $\mathcal{P}_i$ est vraie, il existe $x_0 \in \mathbb{Z}$ tel que $a \equiv x_0^2 \pmod{p^i}$. On veut montrer qu'il existe $x_1 \in \mathbb{Z}$ tel que $a = x_1^2 \pmod{p^{i+1}}$, on cherche x_1 sous la forme $x_1 = x_0 + p^i t$. On a :

$$\begin{aligned} x_1^2 &= x_0^2 + 2p^i x_0 t + p^{2i} t^2 \\ &\equiv x_0^2 + 2p^i x_0 t \pmod{p^{i+1}} \end{aligned}$$

Or $\bar{2}$ et $\bar{x_0}$ sont inversibles dans $\mathbb{Z}/p\mathbb{Z}$ et par hypothèse p^i divise $a^2 - x_0^2$ donc en posant $t = \dfrac{a - x_0^2}{2p^i x_0}$ et $x_1 = x_0 + p^i t$ on a $a = x_1^2 \pmod{p^{i+1}}$ (car $x_1^2 = a + \frac{(a-x_0^2)^2}{4x_0^2}$ et $a - x_0^2$ est un multiple de p^i).
Suposons maintenant $p = 2$ et $a \equiv 1 \pmod 8$ alors on a aussi $a \equiv 1 \pmod 4$ et comme 1 est un carré modulo 4 et 8, $\mathcal{P}_2$ et $\mathcal{P}_3$ sont vraies. Soit alors un entier $i \geqslant 3$ tel que $\mathcal{P}_i$ est vraie. Il existe alors $(x_0, k) \in \mathbb{Z}^2$ tel que $a = x_0^2 + k2^i$. On pose $x_1 = x_0 + 2^{i-1}t$ avec $t = \frac{a-x_0^2}{2^i x_0}$ et on a : $x_1^2 = \left(x_0 + \frac{a-x_0^2}{2x_0}\right)^2 = a^+ \frac{(a-x_0^2)^2}{4x_0^2} = a^+ \frac{k^2}{x_0} 2^{2i-2}$ avec $2i - 2 \geqslant i + 1$ car $i \geqslant 3$ donc $x_1^2 \equiv a \pmod{2^{i+1}}$.
Ceci achève la récurrence. ◪

Nous allons dans la suite du projet étudier «localement» l'équation (1.1).

Chapitre 3

Rappels et compléments concernant les nombres p-adiques.

Les parties 3.1 et 3.2 sont composées de rappels, essentiellement sans démonstration, concernant les nombres p-adiques. Dans tout ce chapitre, p désigne un nombre premier.

3.1 L'anneau $\mathbb{Z}_p$ et le corps $\mathbb{Q}_p$.

Pour tout entier $n \geqslant 1$, on pose $A_n = \mathbb{Z}/p^n\mathbb{Z}$. Étant donné un élément de A_{n+1} on peut considérer un de ses relèvements dans $\mathbb{Z}$ puis sa projection dans A_n, on obtient ainsi un morphisme d'anneaux

$$\phi_{n+1} : A_{n+1} \to A_n$$

qui est surjectif, de noyau $p^n A_{n+1}$.

Définition 1 *On appelle anneau des entiers p-adiques, et on note $\mathbb{Z}_p$, la limite projective du système $(A_n, \phi_n)_{n\geqslant 1}$. Ainsi un élément $x \in \mathbb{Z}_p$ est une suite $(x_n)_{n\geqslant 1} \in \prod_{n=1}^{\infty} A_n$ telle que $\phi_n(x_n) = x_{n-1}$ si $n \geqslant 2$. L'addition et la multiplication de $\mathbb{Z}_p$ sont définies coordonnées par coordonnées.*

Définition 2 *On appelle groupe des unités p-adiques le groupe multiplicatif $\mathcal{U} := \mathbb{Z}_p^{\times}$, et pour tout $n \geqslant 1$, on pose $\mathcal{U}_n = 1 + p^n\mathbb{Z}_p$.*

Proposition 4 *Pour tout $n \in \mathbb{N}^*$ on a l'isomorphime d'anneaux suivant : $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$.*

Proposition 5 *Pour qu'un élément de $\mathbb{Z}_p$ (resp. A_n) soit invesrible, il faut et il suffit qu'il ne soit pas divisible par p. De plus, tout élément non nul x de $\mathbb{Z}_p$ s'écrit de façon unique sous la forme $x = p^k u$ avec $k \in \mathbb{N}$ et $u \in \mathcal{U}$.*

L'entier k de la proposition précédente s'appelle la valuation p-adique de x et se note $v_p(x)$. On pose $v_p(0) = +\infty$, et pour tout $x, y \in \mathbb{Z}_p$ on a :

$$\begin{aligned} v_p(xy) &= v_p(x) + v_p(y) \\ v_p(x+y) &\geqslant \inf(v_p(x), v_p(y)) \\ v_p(x+y) &= \inf(v_p(x), v_p(y)) \text{ si } v_p(x) \neq v_p(y). \end{aligned}$$

La première formule montre que $\mathbb{Z}_p$ est intègre.

On munit les A_n de la topologie discrête et $\mathbb{Z}_p$ de la topologie produit.

Proposition 6 *La topologie de $\mathbb{Z}_p$ peut être définie par la distance*

$$d(x,y) = p^{-v_p(x-y)}.$$

L'anneau $\mathbb{Z}_p$ est un espace compact, complet, dans lequel $\mathbb{Z}$ est dense.

Définition 3 *On appelle corps des nombres p-adiques, et on note $\mathbb{Q}_p$, le corps des fractions de l'anneau $\mathbb{Z}_p$.*

On a $\mathbb{Q}_p = \mathbb{Z}_p[p^{-1}]$ et tout élément $x \in \mathbb{Q}_p^*$ s'écrit de façon unique sous la forme $p^n u$ avec $n \in \mathbb{Z}$ et $u \in \mathcal{U}$. L'entier n s'appelle la valuation p-adique de x et se note $v_p(x)$. On a $v_p(x) \geqslant 0$ si et seulement si $x \in \mathbb{Z}_p$; et si x est un carré dans $\mathbb{Q}_p$ alors $v_p(x)$ est pair.

Proposition 7 *Le corps $\mathbb{Q}_p$ muni de la topologie définie par la distance $d(x,y) = p^{-v_p(x-y)}$ est localement compact et $\mathbb{Z}_p$ en est un sous-anneau ouvert; le corps $\mathbb{Q}$ est dense dans $\mathbb{Q}_p$.*

3.2 Équations p-adiques.

Dans cette partie nous nous intéressons équations $f(x_1,\dots,x_m) = 0$ où $f \in \mathbb{Z}_p[X_1,\dots,X_m]$, $m \in \mathbb{N}^*$ et p premier. On dit que $x = (x_1,\dots,x_m) \in \mathbb{Z}_p^m$ est primitif s'il existe $i \in [\![1,m]\!]$ tel que x_i est inversible, c'est-à-dire que x_i n'est pas divisible par p. Nous donnons une preuve des résultats que nous utiliserons par la suite.

Proposition 8 *Soit $f \in \mathbb{Z}_p[X_1,\dots,X_m]$ un polynôme homogène. Alors f a un zéro non trivial dans $\mathbb{Q}_p^m$ si et seulement si f a un zéro primitif dans $\mathbb{Z}_p^m$.*

Démonstration :
Supposons qu'il existe $x = (x_1,\dots,x_m) \in \mathbb{Q}_p^m/\{(0,\dots,0)\}$ tel que $f(x) = 0$. On pose $h := \min(v_p(x_1),\dots,v_p(x_m))$ ($h < +\infty$ car $x \neq 0$) et $y = p^{-h}x$. Alors y est un élément primitif de $\mathbb{Z}_p^m$ et $f(y) = 0$. La réciproque est évidente.

Le lemme suivant est l'analogue p-adique de la méthode de Newton.

Lemme 2 *Soit $f \in \mathbb{Z}_p[X]$. Soient $x \in \mathbb{Z}_p$ et $n,k \in \mathbb{N}$ tels que $0 \leqslant 2k < n$, $f(x) \equiv 0 \pmod{p}^n$ et $v_p(f'(x)) = k$. Il existe $y \in \mathbb{Z}_p$ tel que :*

$$\begin{aligned} f(y) &\equiv 0 \pmod{p^{n+1}} \\ v_p(f'(y)) = k \quad &et \quad y \equiv x \pmod{p^{n-k}}. \end{aligned}$$

Le théorème suivant permet de demontrer l'existence d'une racine d'un polynôme à plusieurs indéterminées sur $\mathbb{Z}_p$.

Théorème 1 (Lemme de Hensel) *Soient $f \in \mathbb{Z}_p[X_1,\dots,X_m]$, $x = (x_1,\dots,x_m) \in \mathbb{Z}_p^m$, $n,k \in \mathbb{N}$ et $j \in [\![1,m]\!]$. On suppose que $0 \leqslant 2k < n$, $f(x) \equiv 0 \pmod{p^n}$ et $v_p(\dfrac{\partial f}{\partial X_j}(x)) = k$.*

Alors il existe $y \in \mathbb{Z}_p^m$ tel que $f(y) = 0$ et $y \equiv x \pmod{p^{n-k}}$ (on dit que x se relève en une solution exacte).

Corollaire 1 *Supposons $p \neq 2$. Soit f une forme quadratique sur $\mathbb{Q}_p$ à coefficients dans $\mathbb{Z}_p$,*

$$f(X_1,\dots,X_m) = \sum_{1 \leqslant i,j \leqslant m} a_{i,j} X_i X_j \in \mathbb{Z}_p[X_1,\dots,X_m] \quad avec\ a_{i,j} = a_{j,i},$$

dont le discriminant $det((a_{i,j})_{1 \leqslant i,j \leqslant m})$ est inversible. Soit $a \in \mathbb{Z}_p$. Toute solution primitive de l'équation $f(x) \equiv a \pmod{p}$ se relève en une solution exacte.

Démonstration :
Soit $x \in \mathbb{Z}_p^m$ primitif tel que $f(x) - a \equiv 0 \pmod{p}$. Les dérivées partielles de $f - a$ sont, pour $j \in [\![1, \ldots, m]\!]$,

$$\frac{\partial(f-a)}{\partial X_j} = 2\sum_{i=1}^{m} a_{i,j} X_i.$$

Mais par hypothèse l'une des composantes de x n'est pas divisible par p, l'un des coefficients $a_{i,j}$ n'est pas divisible par p et $p \neq 2$, donc il existe $j \in [\![1, \ldots, m]\!]$ tel que $\dfrac{\partial(f-a)}{\partial X_j} \not\equiv 0 \pmod{p}$ et par le théorème précédent (appliqué avec $n = 1$ et $k = 0$) x se relève en une solution exacte. ◪

Corollaire 2 *Supposons $p = 2$. Soit f une forme quadratique à coefficients dans $\mathbb{Z}_2$,*

$$f(X_1, \ldots, X_m) = \sum_{1 \leqslant i,j \leqslant m} a_{i,j} X_i X_j \in \mathbb{Z}_2[X_1, \ldots, X_m] \quad \textit{avec } a_{i,j} = a_{j,i},$$

dont de discriminant $det((a_{i,j})_{1 \leqslant i,j \leqslant m})$ est inversible. Soit $a \in \mathbb{Z}_p$. Toute solution primitive de l'équation $f(x) \equiv a \pmod{8}$ se relève en une solution exacte.

Démonstration :
Soit $x \in \mathbb{Z}_2^m$ primitif tel que $f(x) - a \equiv 0 \pmod{8}$. Les dérivées partielles de $f - a$ sont, pour $j \in [\![1, \ldots, m]\!]$,

$$\frac{\partial(f-a)}{\partial X_j} = 2\sum_{i=1}^{m} a_{i,j} X_i.$$

Mais par hypothèse l'une des composantes de x n'est pas divisible par 2 et l'un des coefficients $a_{i,j}$ n'est pas divisible par 2 donc il existe $j \in [\![1, \ldots, m]\!]$ tel que $\dfrac{\partial(f-a)}{\partial X_j} \not\equiv 0 \pmod{4}$ et par le théorème précédent (appliqué avec $n = 3$ et $k = 1$) x se relève en une solution exacte. ◪

3.3 Les carrés de $\mathbb{Q}_p^*$.

On note $\mathbb{Q}_p^{*2} = \{x \in \mathbb{Q}_p^*, \exists y \in \mathbb{Q}_p^* : x = y^2\}$. Les résultats suivants décrivent $\mathbb{Q}_p^{*2}$ et $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.

Théorème 2 *Supposons $p \neq 2$, et soit $x = p^n u \in \mathbb{Q}_p^*$ avec $n \in \mathbb{Z}$ et $u \in \mathcal{U}$. Pour que x soit un carré dans $\mathbb{Q}_p$ il faut et il suffit que n soit pair et que l'image $\bar{u}$ de u dans $\mathcal{U}/\mathcal{U}_1 = \mathbb{F}_p^*$ soit un carré.*

Démonstration :
Écrivons $u = \sum_{k=0}^{+\infty} c_k p^k$ avec $0 \leqslant c_k < p$, et $c_0 \neq 0$. On remarque que $\bar{u} = c_0$. Supposons qu'il existe $y = p^m v \in \mathbb{Q}_p^*$, avec $m \in \mathbb{Z}$ et $v \in \mathcal{U}$, tel que $y^2 = x$. Alors $n = 2m$ donc n est pair et, si $v \equiv b \pmod{p}$, on a $c_0 \equiv b^2 \pmod{p}$. Réciproquement, supposons que $n = 2m$ et $c_0 \equiv b^2 \pmod{p}$ ($b \in \mathbb{Z}^*$). Notons F le polynôme $X^2 - u$; on a $F(b) \equiv 0 \pmod{p}$ et $F'(b) = 2b \not\equiv 0 \pmod{p}$, donc par le lemme de Hensel il existe $v \in \mathbb{Z}_p$ tel que $F(v) = 0$ et $v \equiv b \pmod{p}$. Ainsi $x = (p^m v)^2$. ◪

Corollaire 3 *Si $p \neq 2$ alors le groupe $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et il admet pour système de représentants $\{1, p, u, up\}$ où $u \in \mathcal{U}$ est tel que sont image dans $\mathcal{U}/\mathcal{U}_1$ n'est pas un carré.*

Démonstration :
C'est immédiat.

Théorème 3 *Pour qu'un élément $x = 2^n u \in \mathbb{Q}_2^*$, avec $n \in \mathbb{Z}$ et $u \in \mathcal{U}$, soit un carré dans $\mathbb{Q}_2^*$ il faut et il suffit que n soit pair et que $u \equiv 1 \pmod 8$.*

Démonstration :
Supposons que x soit un carré dans $\mathbb{Q}_2^*$. Alors $n = 2m$ donc n est pair et, comme le carré d'un nombre impair est toujour congru à 1 modulo 8, on a $u \equiv 1 \pmod 8$. Réciproquement, supposons que $n = 2m$ et $u \equiv 1 \pmod 8$. Notons F le polynôme $X^2 - u$; on a $F(1) \equiv 0 \pmod 8$ et $F'(1) = 2 \not\equiv 0 \pmod 4$, donc par le lemme de Hensel il existe $v \in \mathbb{Z}_2$ tel que $F(v) = 0$ et $v \equiv 1 \pmod 4$. Ainsi $x = (p^m v)^2$. ◻

Corollaire 4 *Le groupe $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et il admet pour système de représentants $\{\pm 1, \pm 5, \pm 2, \pm 10\}$.*

Démonstration :
Par le théorème précédent, le système des résidus 1,3,5,7 modulo 8 est un système de représentants des classes résiduelles du quotient du groupe des unités 2-adiques par le sous-groupe de ses carrés. On ajoute alors à ce système les produits de ces résidus par 2.

Théorème 4 *Le groupe $\mathbb{Q}_p^{*2}$ est un sous-groupe ouvert de $\mathbb{Q}_p^*$.*

Démonstration :
Cela résulte des théorèmes 2 et 3. Soit $x = p^n u \in \mathbb{Q}_p^{*2}$ avec $n \in \mathbb{Z}$ et $u \in \mathcal{U}$. Supposons d'abord $p \neq 2$. Notons B la boule ouverte de $\mathbb{Q}_p^*$ de centre x et de rayon p^{-n}. Soit $y = p^m v \in \mathbb{Q}_p^*$, avec $n \in \mathbb{Z}$ et $u \in \mathcal{U}$, tel que $y \in B$. On a donc $d(x, y) < p^{-n}$. Comme la distance que l'on a définie sur $\mathbb{Q}_p$ est ultramétrique, on a nécéssairement $m = n$. Puis, pour que l'inégalité soit stricte, on doit avoir $x \equiv y \pmod p$, donc y est un carré de $\mathbb{Q}_p^*$. Dans le cas où $p = 2$ la démonstation est similaire, il faut juste considérer une boule de rayon plus petit (p^{-n+2}). ◻

Chapitre 4

Symbole de Hilbert.

4.1 Propriétés locales.

Dans ce paragraphe k désigne soit un corps $\mathbb{Q}_p$, soit $\mathbb{R}$.

Définition 4 *Soient $a, b \in k^*$. On pose :*

$$(a,b) = \begin{cases} 1 & \text{si } z^2 - ax^2 - by^2 = 0 \text{ a une solution non nulle dans } k^3 \\ -1 & \text{sinon.} \end{cases}$$

Le nombre (a,b) s'appelle le symbole de Hilbert de a et b, relativement à k.

On voit facilement que symbole de Hilbert définit une application de $k^*/k^{*2} \times k^*/k^{*2}$ dans $\{1,-1\}$.

Proposition 9 *Soient $a, b \in k^*$ et $k_b = k(\sqrt{b})$.*

Pour que $(a,b) = 1$, il faut et il suffit que a apartienne au groupe $N(k_b^*)$ des normes (relativement à k_b/k) des éléments de k_b^*.

Démonstration :
L'extension k_b/k est de degré 1 où 2. Si elle est de degré 1 alors il existe $c \in k^*$ tel que $c^2 = b$ et, d'une part l'équation $z^2 - ax^2 - by^2 = 0$ admet pour solution $(c,0,1)$ donc $(a,b) = 1$, d'autre part $a \in k^* = N(k_b^*)$. Supposons maintenant que $[k_b : k] = 2$ et désignons par β une racine carré de b. Si $a \in N(k_b^*)$ alors il existe $s, t \in k$ tels que $a = s^2 - bt^2$ et alors $(s,1,t)$ est solution de l'équation $z^2 - ax^2 - by^2 = 0$ donc $(a,b) = 1$. Réciproquement, si $(a,b) = 1$ alors il existe $(x,y,z) \in k^3 \backslash \{(0,0,0)\}$ tel que $z^2 - ax^2 - by^2 = 0$, et $x \neq 0$ sinon b serait un carré et l'extension serait de degré 1 ; on en conclut que a est norme de $\frac{z}{x} + \beta\frac{y}{x}$. ◪

Proposition 10 *Pour tout $a, a', b \in K$ le symbole de Hilbert vérifie :*

1) $(a,b) = (b,a)$ *et* $(a,b^2) = 1$;

2) $(a,-a) = 1$ *et* $(a,1-a) = 1$;

3) si $(a,b) = 1$ *alors* $(aa',b) = (a',b)$;

4) $(a,b) = (a,-ab) = (a,(1-a)b)$.

Démonstration :
La formule 1) est évidente. Pour démontrer la formule 2) il suffit de remarquer que si $b = -a$ (resp. $b = 1-a$) alors l'équation $z^2 - ax^2 - by^2 = 0$ a pour solution $(0,1,1)$ (resp. $(1,1,1)$) ; on a donc $(a,b) = 1$. Passons à 3). Si $(a,b) = 1$ alors, d'après la proposition 9, on a $a \in N(k_b^*)$; par multiplicativité de la norme on a $a' \in N(k_b^*)$ si et seulement si $aa' \in N(k_b^*)$, ce qui démontre 3). Enfin 4) résulte de 1), 2) et 3). ◪

Lemme 3 *Soit $v \in \mathcal{U}$ et supposons que l'équation $z^2 - px^2 - vy^2 = 0$ a une solution non triviale dans $\mathbb{Q}_p^3$. Alors elle a une solution (z, x, y) telle que $z, y \in \mathcal{U}$ et $x \in \mathbb{Z}_p$.*

Démonstration :
D'après la proposition 8, l'équation considérée a une solution primitive (z, x, y). Montrons que $z, y \in \mathcal{U}$. Supposons que ce ne soit pas le cas, c'est-à-dire que p divise y ou z. Alors $z^2 - vy^2 \equiv 0 \pmod p$, mais $v \not\equiv 0 \pmod p$, donc $y \equiv 0 \pmod p$ et $z \equiv 0 \pmod p$, d'où $px^2 \equiv 0 \pmod{p^2}$, ce qui montre que p divise aussi x contrairement au caractère primitif de (z, x, y). ◲

Définition 5 *On définit deux fonctions, ϵ et ω respectivement de l'ensemble des entiers impairs dans $\mathbb{Z}/2\mathbb{Z}$ par les formules :*

$$\epsilon(n) \equiv \frac{n-1}{2} \pmod 2 = \begin{cases} \bar{0} & si\ n \equiv\ 1 \pmod 4 \\ \bar{1} & si\ n \equiv -1 \pmod 4 \end{cases}$$

$$\omega(n) \equiv \frac{n^2-1}{8} \pmod 2 = \begin{cases} \bar{0} & si\ n \equiv \pm 1 \pmod 8 \\ \bar{1} & si\ n \equiv \pm 5 \pmod 8 \end{cases}$$

Proposition 11 *Les fonctions ϵ et ω sont des morphismes de groupes respectivement de $(\mathbb{Z}/4\mathbb{Z})^\times$, $(\mathbb{Z}/8\mathbb{Z})^\times$ sur $\mathbb{Z}/2\mathbb{Z}$.*

Démonstration :
La vérification est immédiate.

Théorème 5 *Si $k = \mathbb{R}$ alors on a $(a, b) = 1$ si et seulement si a ou b est strictement positif.*
Si $k = \mathbb{Q}_p$ et si on écrit $a = p^\alpha u, b = p^\beta v$ avec $u, v \in \mathcal{U}$ alors on a :
$(a, b) = (-1)^{\alpha\beta\epsilon(p)} (\frac{u}{p})^\beta (\frac{v}{p})^\alpha$ *si $p \neq 2$;*

$(a, b) = (-1)^{\epsilon(u)\epsilon(v) + \alpha\omega(v) + \beta\omega(u)}$ *si $p = 2$;*
où on a noté $(\frac{u}{p})$ le symbole de Legendre $(\frac{\bar{u}}{p})$ où $\bar{u}$ désigne la réduction de u dans $\mathcal{U}/\mathcal{U}_1 \simeq \mathbb{F}_p^*$; et $\epsilon(u), \omega(u)$ désignent respectivement la classe modulo 2 de $\dfrac{u-1}{2}$ et de $\dfrac{u^2-1}{8}$.

Démonstration :
Le cas où $k = \mathbb{R}$ est trivial. On suppose maintenant que $k = \mathbb{Q}_p$ avec $p \neq 2$. Il est clair que les exposants α et β n'interviennent que par leur résidu modulo 2, et par symétrie du symbole de Hilbert il n'y a que trois cas à considérer : $(\alpha, \beta) \in \{(0, 0), (1, 0), (1, 1)\}$.

Supposons que $\alpha = 0, \beta = 0$. Il faut vérifier que $(u, v) = 1$. Considérons la forme quadratique f sur $\mathbb{Q}_p$ définie par $f(X_1, X_2, X_3) = X_1^2 - uX_2^2 - vX_3^2$, son discriminant est $uv \in \mathcal{U}$. Notons $\pi : \mathbb{Z}_p \to \mathbb{Z}/p\mathbb{Z}$ l'application qui a $x \in \mathbb{Z}_p$ associe sa première composante. Par le corollaire 1, pour montrer que $(u, v) = 1$ il suffit de montrer que l'équation $z^2 - \pi(u)x^2 - \pi(v)y^2 = 0$ a une solution non nul dans $\mathbb{F}_p^3$. Fixons $z \in \mathbb{F}_p^*$. Comme u et v sont dans $\mathcal{U}$, les nombres $\pi(u)$ et $\pi(v)$ sont dans $\mathbb{F}_p^*$, et les ensembles $A := \{z^2 - \pi(u)x^2, x \in \mathbb{F}_p\}$ et $B := \{\pi(v)y^2, y \in \mathbb{F}_p\}$ sont en bijection avec l'ensenble des carrés de $\mathbb{F}_p$, ils sont donc de cardinal $\frac{p+1}{2}$, or $\frac{p+1}{2} + \frac{p+1}{2} = p + 1 > p = |\mathbb{F}_p|$ donc les ensembles A et B ne peuvent être disjoints et l'équation $z^2 - \pi(u)x^2 - \pi(v)y^2 = 0$ a une solution non nul dans $\mathbb{F}_p^3$.

Supposons que $\alpha = 1, \beta = 0$. Il faut vérifier que $(pu, v) = (\frac{v}{p})$. D'après le cas précédent on a $(u, v) = 1$, et d'après la proposition 10 3) on a alors $(pu, v) = (p, v)$. Il suffit donc de vérifier que $(p, v) = (\frac{v}{p})$. C'est immédiat si v est un carré dans $\mathbb{Z}_p$, les deux termes étant égaux à 1. Sinon on a $(\frac{v}{p}) = -1$ et nous allons montrer au moyen du lemme 3 que $(p, v) = -1$. Supposons que $(p, v) = 1$, alors par le lemme 3 il existe (z, x, y) avec

$z, y \in \mathcal{U}$ et $x \in \mathbb{Z}_p$ tel que $z^2 - px^2 - vy^2 = 0$. On a alors $v = (\frac{y}{z})^2(1 - p(\frac{z}{y})^2(\frac{x}{y})^2)$ ce qui montre que $(\frac{v}{p}) = 1$. Finalement on a bien $(p, v) = (\frac{v}{p})$.

Supposons que $\alpha = 1, \beta = 1$. Il faut vérifier que $(pu, pv) = (-1)^{(p-1)/2}(\frac{u}{p})(\frac{v}{p})$. Or les formules 4) et 1) de le proposition 10 montre que $(pu, pv) = (pu, -p^2uv) = (pu, -uv)$. On utilise ensuite le cas précédent, la linéarité du symbole de hilbert et le fait que $(\frac{-1}{p}) = (-1)^{(p-1)/2}$ pour écrire :

$$(pu, pv) = (\frac{-uv}{p}) = (\frac{-1}{p})(\frac{u}{p})(\frac{v}{p}) = (-1)^{(p-1)/2}(\frac{u}{p})(\frac{v}{p}).$$

On passe maintenant au cas de $\mathbb{Q}_2$. Ici encore, α et β n'interviennent que par leur résidu modulo 2, et il y a trois cas à considérer.

Supposons $\alpha = 0, \beta = 0$. Il faut vérifier que $(u, v) = 1$ si u ou v est congru à 1 modulo 4, et que $(u, v) = -1$ sinon. Supposons $u \equiv 1 \pmod 4$ (u et v jouent des rôles symétriques), on a alors $u \equiv 1 \pmod 8$ ou $u \equiv 5 \pmod 8$. Dans le premier cas u est un carré dans $\mathbb{Q}_2$ d'après le théorème 3 et alors $(u, v) = 1$. Dans le second cas $u + av$ est un carré dans $\mathbb{Q}_2$ car $u + av \equiv 5 + 4 \equiv 1 \pmod 8$, il existe donc $w \in \mathcal{U}$ tel que $w^2 = u + 4v$ et alors $(w, 1, 2)$ est une solution non nulle de l'équation $z^2 - ux^2 - vy^2 = 0$ et on a bien $(u, v) = 1$. Supposons maintenant que u et v ne sont pas congrus à 1 modulo 4, alors il sont congru à -1 modulo 4 car ce sont des unités 2-adiques. Nous allons montrer que $(u, v) = -1$ par le lemme 3. Si (z, x, y) est une solution primitive de l'équation $z^2 - ux^2 - vy^2 = 0$ alors on a $z^2 + x^2 + y^2 \equiv 0 \pmod 4$, mais les carrés de $\mathbb{Z}/4\mathbb{Z}$ sont 0 et 1 donc on doit avoir x, y, z congrus à 0 modulo 2, contrairement à l'hypothèse de primitivité. On a donc bien $(u, v) = -1$ dans ce cas.

Supposons $\alpha = 1, \beta = 0$. Il faut vérifier que $(2u, v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(v)}$. Nous allons montrer que $(2u, v) = (2, v)(u, v)$ et que $(2, v) = (-1)^{\omega(v)}$ (par le cas précédent on a déjà $(u, v) = (-1)^{\epsilon(u)\epsilon(v)}$). On commence par montrer que $(2, v) = (-1)^{\omega(v)}$ c'est-à-dire que $(2, v) = 1$ si et seulement si $v \equiv \pm 1 \pmod 8$. D'après le lemme 3, si $(2, v) = 1$ alors il existe $x, y, z \in \mathbb{Z}_2$ tels que $z^2 - 2x^2 - vy^2 = 0$ et $y, z \in \mathcal{U}$. On a $y^2 \equiv z^2 \equiv 1 \pmod 8$ (car ce sont des carré dans $\mathbb{Z}_2$), d'où $v \equiv 1 - 2x^2 \pmod 8$. Mais les carrés de $\mathbb{Z}/8\mathbb{Z}$ sont 0,1 et 4, donc $v \equiv \pm 1 \pmod 8$. Réciproquement, si $v \equiv 1 \pmod 8$ alors v est un carré dans $\mathbb{Q}_2$ et $(2, v) = 1$; si $v \equiv -1 \pmod 8$, alors $-v$ est un carré de $\mathbb{Q}_2$ donc $(2, -v) = 1$ et par la proposition 10 on a $(2, v) = (2, -v^2) = (2, -1)$ or l'équation $z^2 - 2x^2 + y^2 = 0$ a pour solution $(1, 1, 1) \in \mathbb{Q}_2^{*3}$ donc $(2, v) = 1$. Il reste à montrer que $(2u, v) = (2, v)(u, v)$. D'après la proposition 10 c'est vrai si $(2, v) = 1$ ou $(u, v) = 1$). Il rest donc à vérifier le cas où $(2, v) = (u, v) = -1$. Dans ce cas on a alors $v \equiv 3 \pmod 8$ d'après ce que l'on vient de démontrer, et u est congru à 3 ou -1 modulo 8 car il ne doit pas être un carré dans $\mathbb{Q}_2$. On peut écrire $v = 3s^2$ où $s \in \mathbb{Q}_2^*$; en effet, comme $\mathcal{U}$ est un groupe on a $w := 3v^{-1} \in \mathcal{U}$ donc $v = 3w^{-1}$, mais $v \equiv 3 \pmod 8$ donc $w^{-1} \equiv 1 \pmod 8$, ainsi w^{-1} est un carré. De même on peut écrire $u = 3t^2$, $u = -t'^2$, $v = -5s'^2$ avec $t, t', s' \in \mathbb{Q}_2^*$, et par la proposition 10 on a alors $(u, v) = (-1, 3)$ ou $(u, v) = (3, -5)$. Or les équations $z^2 + 2x^2 - 3y^2 = 0$ et $z^2 - 6x^2 + 5y^2 = 0$ ont pour solution $(1, 1, 1)$ donc on a bien $(u, v) = 1$.

Supposons maintenant $\alpha = 1, \beta = 1$. Il faut vérifier que $(2u, 2v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(u)+\omega(v)}$. Or, d'après la proposition 10, le cas précédent et la proposition 11 on a :

$$\begin{aligned}(2u, 2v) = (2u, -4uv) = (2u, -uv) &= (-1)^{\epsilon(u)\epsilon(-uv)+\omega(-uv)} \\ &= (-1)^{\epsilon(u)(\epsilon(-1)+\epsilon(u)+\epsilon(v))+\omega(-1)+\omega(u)+\omega(v)}\end{aligned}$$

Or $-1 = (1, 3, 7, \dots)$ donc $\epsilon(-1) = 1, \omega(-1) = 0$ et $\epsilon(u)(1 + \epsilon(u)) = 0$, d'où la formule attendue. ◲

Théorème 6 *Le symbole de Hilbert est une forme bilinéaire non dégénérée sur le $\mathbb{F}_2$-espace vectoriel k^*/k^{*2}.*

Démonstration :
La bilinéarité résulte immédiatement des formules du théorème précédent et du fait que ϵ et ω sont des morphismes. Pour montrer que cette forme est non dégénérée il suffit d'exhiber pour chaque $a \in k^*/k^{*2}\backslash\{1\}$

un élément b tel que $(a,b)=-1$. Nous avons indiqué des systèmes de représentants pour les différents $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ aux théorèmes 3 et 4. Dans le cas $p\neq 2$ on considère $u\in\mathcal{U}$ tel que $(\frac{u}{p})=-1$ et pour a valant successivement p,u,up on prend pour b respectivement u,p,u. Dans le cas de $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ on remarque que pour $u\in\{1,5,-1,-5\}$ on a $2u\in\{2,6,-2,-6\}$ et que $(5,2u)=-1$ (car $\epsilon(5)=0$ et $\omega(5)=1$), $(-1,-1)=(-1,-5)=-1$. ◪

4.2 Propriétés globales.

Le corps $\mathbb{Q}$ se plonge comme sous-corps dense dans chacun des corps $\mathbb{Q}_p$ et $\mathbb{R}$. Si $a,b\in\mathbb{Q}^*$ on note $(a,b)_p$ (resp. $(a,b)_\infty$) le symbole de Hilbert de leurs images dans $\mathbb{Q}_p$ (resp. $\mathbb{R}$). On désigne par V la réunion de l'ensemble des nombre premiers et du symbole ∞, et on note $\mathbb{Q}_\infty=\mathbb{R}$.

Théorème 7 (Formule du produit.) *Si $a,b\in\mathbb{Q}^*$, alors on a $(a,b)_v=1$ pour presque tout $v\in V$ et*

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

Démonstration :
Puisque les symboles de Hilbert sont bilinéaires il suffit de démontrer la formule du produit lorsque a et b sont égaux à -1 ou a un nombre premier. On utilisera le théorème 5 dans chaque cas. Notons l et l' deux nombres premiers.

Si $a=b=-1$, alors on a $(-1,-1)_\infty=(-1,-1)_2=-1$ et $(-1,-1)_v=1$ pour $v\in V\backslash\{2,\infty\}$, et le produit est bien égal à 1.

Supposons que $a=-1$ et $b=l$. Si $l=2$ alors on a $(-1,2)_v=1$ pour tout $v\in V$. Si $l\neq 2$ alors on a $(-1,l)_v=1$ pour tout $v\in V\backslash\{2,l\}$ et $(-1,l)_2=(-1,l)_l=(-1)^{\epsilon(l)}$ et le produit est bien égal à 1.

Supposons que $a=l$ et $b=l'$. Si $l=l'$ alors, par la formule 4) de la proposition 10, on a $(l,l)_v=(-1,l)_v$ pour tout $v\in V$ et on est ramené au cas précédent. Supposons maintenant que $l\neq l'$. Si $l'=2$ alors on a $(l,2)_v=1$ pour tout $v\in V\backslash\{2,l\}$ et $(l,2)_2=(-1)^{\omega(l)}$, $(l,2)_l=(\frac{2}{l})=(-1)^{\omega(l)}$, donc le produit vaut bien 1. Si l et l' sont distincts et différent de 2, alors on a $(l,l')_v=1$ pour tout $v\in V\backslash\{2,l,l'\}$ et

$$(l,l')_2=(-1)^{\epsilon(l)\epsilon(l')},\ (l,l')_l=(\frac{l'}{l}),\ (l,l')_{l'}=(\frac{l}{l'});$$

mais d'après la loi de réciprocité quadratique on a $(\frac{l'}{l})(\frac{l}{l'})=(-1)^{\epsilon(l)\epsilon(l')}$, donc le produit est bien égal à 1. ◪

Lemme 4 (lemme d'aproximation) *Soit S une partie finie de V. L'image de $\mathbb{Q}$ dans $\prod_{v\in S}\mathbb{Q}_v$ est dense dans ce produit (pour la topologie produit de celles des $\mathbb{Q}_v$).*

Démonstration :
Quitte a agrandir S on peut supposer que $\infty\in S$, on note alors $S=\{\infty,p_1,\dots,p_n\}$ où les p_i sont des nombres premiers distincts. Il s'agit de montrer que $\mathbb{Q}$ est dense dans $\mathbb{R}\times\mathbb{Q}_{p_1}\times\cdots\times\mathbb{Q}_{p_n}$ mais comme $\mathbb{Z}_{p_i}$ est dense dans $\mathbb{Q}_{p_i}$ pour tout $i=1,\dots,n$, il suffit de montrer que $\mathbb{Q}$ est dense dans $A:=\mathbb{R}\times\mathbb{Z}_{p_1}\times\cdots\times\mathbb{Z}_{p_n}$. Soit $(x_\infty,x_1,\dots,x_n)\in A$, et fixons un réel $\epsilon>0$ et un entier $N\geqslant 0$. On cherche $x\in\mathbb{Q}$ tel que :

$$|x-x_\infty|\leqslant\epsilon \text{ et } v_{p_i}(x-x_i)\geqslant N \text{pour tout } i=1,\dots,n.$$

Comme les p_i sont distincts, le lemme chinois in dique qu'il existe $x_0\in\mathbb{Z}$ tel que $x_0\equiv x_i\pmod{p_i^N}$ pour tout $i=0,\dots,N$; on a alors $v_{p_i}(x_0-x_i)\geqslant N$ pour tout $i=0,\dots,N$. Soit q un nombre premier n'appartenant pas a S. L'ensemble $B:=\{\frac{a}{q^m},a\in\mathbb{Z},m\in\mathbb{N}^*\}$ est dense dans $\mathbb{R}$ (la démonstration est similaire à celle de la densité des nombres décimaux dans $\mathbb{R}$). On peut donc choisir $u\in B$ tel que :

$$|x_0-x_\infty+up_1^N\dots p_n^N|\leqslant\epsilon.$$

Le nombre rationnel $x_0+up_1^N\dots p_n^N$ est alors solution du problème. ◪

Le résultat suivant est admis.

Lemme 5 (progression arithmétique (Dirichlet)) *Soient a et m deux entiers strictement positifs premiers entre eux. Il existe une infinité de nombres premiers p tels que $p \equiv a \pmod m$.*

Théorème 8 *Soit $(a_i)_{i\in I}$ une famille finie d'éléments de $\mathbb{Q}^*$ et soit $(\epsilon_{i,v})_{i\in V, v\in V})$ une famille de nombres appartenant à $\{1,-1\}$. Pour qu'il existe $x \in \mathbb{Q}^*$ tel que $(a_i,x)_v = \epsilon_{i,v}$ pour tout $i \in V$ et $v \in V$, il faut et il suffit que les trois conditions suivantes soient vérifiées :*

1) presque tous les $\epsilon_{i,v}$ sont égaux à 1 ;

2) pour tout $i \in I$, $\prod_{v\in V} \epsilon_{i,v} = 1$;

3) pour tout $v \in V$, il existe $x_v \in \mathbb{Q}_v^*$, tel que pour tout $i \in I$ on ait :$(a_i, x_v)_v = \epsilon_{i,v}$.

Démonstration :
La nécessité de 1) et 2) résulte de la formule du produit ; celle de 3) est triviale (prendre $x_v = x$). Réciproquement, on suppose que la famille $(\epsilon_{i,v})_{i\in V, v\in V})$ vérifie 1), 2) et 3). Par la proposition 10, quitte à multiplier les a_i par le carré d'un entier, on peut supposer que tous les a_i sont entiers. Soit S le sous-ensemble de V formé de $\infty, 2$ et des facteurs premiers des a_i, et soit $T := \{v \in V, \exists i \in I, \epsilon_{i,v} = -1\}$. Les ensembles S et T sont clairement finis. On distingue deux cas.

Supposons pour l'instant que $S \cap T = \varnothing$. Posons :

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

Puisque $S \cap T = \varnothing$ et que 2 ne divise pas a, les entiers a et m sont premiers entre eux, et, d'après le théorème de la progression arithmétique, il existe un nombre premier p tel que $p \equiv a \pmod m$. En particulier p ne divise ni a ni m, donc $p \notin S \cup T$. Nous allons voir que $x := ap$ est solution du problème c'est-à-dire que $(a_i, x)_v = \epsilon_{i,v}$ pour tout $(i, v) \in I \times V$.

Supposons d'abord que $v \in S$, on a alors $\epsilon_{i,v} = 1$ puisque $S \cap T = \varnothing$, et il faut vérifier que $(a_i, x)_v = 1$ pour tout $i \in I$. Cela est vrai si $v = \infty$ car $x > 0$. Si v est un nombre premier l, on a $x = ap \equiv a^2 \pmod m$, d'où $x \equiv a^2 \pmod 8$ (car 8 divise m) et $x \equiv a^2 \pmod l$ (car l divise m). Or a est une unité l-adique (car $l \notin T$), p est une unité l-adique (car $p \notin S$ et $l \in S$) donc x est aussi une unité l-adique ; les théorèmes 2 et 3 montrent alors que x est un carré dans $\mathbb{Q}_l^*$ et on a bien $(a_i, x)_v = 1$. Supposons maintenant que $v = l \notin S$; alors pour tout $i \in I$, a_i est une unité l-adique. Comme $l \neq 2$ on a :

$$(a_i, b)_l = \left(\frac{a_i}{l}\right)^{v_l(b)} \quad \text{pour tout } b \in \mathbb{Q}_l^*.$$

Si $l \notin T \cup \{p\}$, alors x est une unité l-adique, donc $v_l(x) = 0$ et la formule ci-dessus montre que $(a_i, x)_l = 1$; d'autre part, on a $\epsilon_{i,l} = 1$ puisque $l \notin T$. Si $l \in T$, on a $v_l(x) = 1$; d'autre part la condition 3) montre qu'il existe $x_l \in \mathbb{Q}_l^*$ tel que $(a_i, x_l) = \epsilon_{i,l}$ pour tout $i \in I$. Comme $l \in T$ il existe $j \in I$ tel que $\epsilon_{j,l} = -1$ et on a $v_l(x_l) \equiv 1 \pmod 2$, d'où :

$$(a_i, x)_l = \left(\frac{a_i}{l}\right) = (a_i, x_l)_l = \epsilon_{i,l} \quad \text{pour tout } i \in I.$$

On considère enfin le cas où $l = p$, que l'on ramène aux autres grâce à la formule du produit :

$$(a_i, x)_p = \prod_{v\in V\setminus\{p\}} (a_i, x)_v = \prod_{v\in V\setminus\{p\}} \epsilon_{i,v} = \epsilon_{i,p}.$$

Cela achève le cas où $S \cap T = \varnothing$.

On passe maintenant au cas général. Les carré de $\mathbb{Q}_v^*$ forment un sous-groupe ouvert de $\mathbb{Q}_p^*$ (cf. théorème 4) donc, d'après le lemme 4, il existe $x' \in \mathbb{Q}^*$ tel que pour tout $v \in S$, x'/x_v soit un carré dans $\mathbb{Q}_v^*$. On a en particulier :

$$(a_i, x')_v = (a_i, x_v)_v = \epsilon_{i,v} \text{ pour tout } v \in S.$$

Posons alors, pour tout $i \in I$ et $v \in V$, $\eta_{i,v} = \epsilon_{i,v}(a_i, x')_v$. La famille $(\eta_{i,v})_{i,v})$ vérifie les conditions $1), 2), 3)$ (pour 1) et 2) on utilise la formule du produit, et pour 3) on considère $x'x_v$), et en plus on a $i, v = 1$ si $v \in S$. Par le cas précédent il existe $y\mathbb{Q}^*$ tel que $(a_i, y)_v = \eta_{i,v}$ pour tout $i \in I$ et tout $v \in V$. Alors il est clair que $x := yx'$ vérifie $(a_i, x)_v = \epsilon_{i,v}$ pour tout $i \in V$ et $v \in V$. ◹

Chapitre 5

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

5.1 Résultats généraux sur les formes quadratiques.

Nous ne rappelerons pas tous les résultats sur les formes quadratiques, on suppose connu les notions de formes quadratiques sur un $\mathbb{K}$-espace vectoriel où $\mathbb{K}$ est un corps, d'orthogonalité, d'isotropie. Nous citons seulement quelques résultats liés aux plans hyperboliques et un théorème sur les bases «contiguës» (c'est-à-dire qui ont un élément en commun). Nous considérons un espace quadratique (k^n, f) de dimension finie n sur un corps k de caractéristique 0, la forme bilinéaire associée à la forme quadratique f est noté $< ., . >$. Si f' est une forme quadratique sur k^n équivalente à f on note $f \sim f'$.

Définition 6 *On appelle plan hyperbolique tout espace quadratique ayant une base formée de deux éléments isotropes x, y tels que $< x, y >\neq 0$. Une forme quadratique f sur k^2 est dite hyperbolique si l'espace quadratique (k^2, f) est hyperbolique.*

Dans la définition précédente, quitte à multiplier y par $\frac{1}{<x,y>}$, on peut même supposer que $< x, y >= 1$.

Proposition 12 *Soit x un élément isotrope non nul d'un espace quadratique non dégénéré $V := (k^n, f)$, où $n \geqslant 2$. Il existe alors un sous-espace U de k^n qui contient x et qui est un plan hyperbolique.*

Corollaire 5 *Si (k^n, f) est non dégénéré de dimension $n \geqslant 2$ et contient un vecteur isotrope non nul alors on a $f(k^n) = k$.*

Définition 7 *On dit qu'une forme quadratique f sur k^n représente $a \in k$ s'il existe $x \in k/\{0\}$ tel que $f(x) = a$.*

Précisons la notation «somme orthogonale» que nous allons employer dans la suite. Si $n, m \in N^*$ et si f et f' sont deux formes quadratiques respectivement sur k^n et k^m, on définit la forme quadratique $f \oplus f'$ sur k^{n+m} par :

$$(f \oplus f')(x_1, \ldots, x_{n+m}) = f(x_1, \ldots, x_n) + f'(x_{n+1}, \ldots, x_{n+m}).$$

On définit aussi $f \ominus f' := f \oplus (-f')$.

Les deux résultats précédents donnent alors la proposition suivante.

Proposition 13 *Si f représente 0 et est non dégénérée alors il existe deux formes quadratiques h et g, avec h hyperbolique, tels que $f \sim h \oplus g$. De plus f représente tout élément de k.*

Corollaire 6 *On suppose $n \geqslant 3$. Soient g une forme quadratique non dégénérée en $n-1$ variables, $a \in k^*$ et aZ^2 la forme quadratique sur $k : z \mapsto az^2$. Les assertions suivantes sont équivalentes :*

1) La forme g représente a.

2) On a $g \sim h \oplus aZ^2$, où h est une forme en $n-2$ variables.

3) La forme $f := g \ominus aZ^2$ représente 0.

Corollaire 7 *Soient g et h deux formes non dégénérées de rang au moins 1, et soit $f := g \ominus h$. Si $a \in k$, on note aZ^2 la forme quadratique sur k : $z \mapsto az^2$. Les assertions suivantes sont équivalentes :*
1) La forme f représente 0.

2) Il existe $a \in k^*$ qui est représenté par g et par h.

3) Il existe $a \in k^*$ tel que $g \ominus aZ^2$ et $h \ominus aZ^2$ représentent 0.

On termine avec un résultat qui nous servira à déterminer un invariant d'une forme quadratique.

Théorème 9 *Supposons V non dégénéré de dimension au moins 3, et soient e= $(e_1, \ldots, e_n)$, $e' = (e'_1, \ldots, e'_n)$ deux bases orthogonales de V. Il existe un entier m et $m+1$ bases orthogonales de V, $e^{(0)}, \ldots, e^{(m)}$, telles que $e^{(0)} = e$, $e^{(m)} = e'$, et telles que $e^{(i)}$ soit contiguë à $e^{(i+1)}$ (c'est-à-dire que ces deux bases ont un éléments en commun) pour $0 \leqslant i < m$.*

5.2 Formes quadratiques sur $\mathbb{Q}_p$.

Dans cette partie p désigne un nombre premier, k désigne un corps $\mathbb{Q}_p$, et f est une forme quadratique non dégénérée sur k. Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base orthogonale de (k^n, f). Notons, pour $i = 1, \ldots, n$, $a_i =< e_i, e_i >$, et posons :

$$\epsilon_f(\mathcal{B}) = \prod_{i<j} (a_i, a_j).$$

On sait déjà que le discriminant de f, $d(f) \in k*/k^{*2}$, est un invariant de f, c'est-à-dire que si f' est une forme quadratique équivalente à f alors $d(f) = d(f')$. Montrons que $\epsilon(\mathcal{B})$ est aussi un invariant de f.

Théorème 10 *Le nombre $\epsilon_f(\mathcal{B})$ ne dépent pas du choix de la base orthogonale $\mathcal{B}$.*

Démonstration :
Notons $\epsilon(\mathcal{B}) = \epsilon_f(\mathcal{B})$. Si $n = 1$ alors $\epsilon(\mathcal{B}) = 1$ pour toute base orthogonale $\mathcal{B}$ de (k, f) (on convient qu'un produit indexé par l'ensemble vide vaut 1). Si $n = 2$ on a les équivalence suivante (on note $\mathcal{B} = (e_1, e_2)$ et $a_1 =< e_1, e_1 >, a_2 =< e_2, e_2 >$) :

$$\begin{aligned} \epsilon(\mathcal{B}) = 1 \Leftrightarrow (a_1, a_2)_p = 1 \Leftrightarrow & \text{ La forme } (Z, X, Y) \mapsto Z^2 - a_1X^2 - a_2Y^2 \text{ représente 0.} \\ \Leftrightarrow & \text{ La forme } (X, Y) \mapsto a_1X^2 + a_2Y^2 \text{ représente 1.} \\ \Leftrightarrow & \text{ Il existe } x \in k^2 \text{ tel que } f(x) = 1. \end{aligned}$$

Mais la dernière assertion ne dépend pas de la base choisie. On raisonne ensuite par récurrence sur $n \in N^*$. Soit $n \geqslant 3$; on suppose que, étant donné un espace quadratique de dimension $n-1$, si $\mathcal{F}$ et $\mathcal{F}'$ sont deux bases orthogonales de cet espace alors $\epsilon(\mathcal{F}) = \epsilon(\mathcal{F}')$. Soient $\mathcal{B} = (e_1, \ldots, e_n)$ et $\mathcal{B}' = (e'_1, \ldots, e'_n)$ deux bases orthogonales de (k^n, f), montrons que $\epsilon(\mathcal{B}) = \epsilon(\mathcal{B}')$. D'après le théorème 9 on peut supposer que $\mathcal{B}$ et $\mathcal{B}'$ sont contiguë. Vu la symétrie du symbole de Hilbert, $\epsilon(\mathcal{B})$ ne change pas si l'on permute des éléments de $\mathcal{B}$, on

peut donc supposer que $e_1 = e'_1$. On note $a_i =< e_i, e_i >$ et $a'_i =< e'_i, e'_i >$ pour $i = 1, \ldots, n$. On a $a_1 = a'_1$ et on peut écrire :

$$\epsilon(\mathcal{B}) = (a_1, a_2 \ldots a_n)_p \prod_{2 \leqslant i < j} (a_i, a_j)_p = (a_1, a_1^2 a_2 \ldots a_n)_p \prod_{2 \leqslant i < j} (a_i, a_j)_p$$
$$= (a_1, a_1 d(f))_p \prod_{2 \leqslant i < j} (a_i, a_j)_p.$$

De même

$$\epsilon(\mathcal{B})' = (a_1, a_1 d(f))_p \prod_{2 \leqslant i < j} (a'_i, a'_j)_p.$$

Mais l'hypothèse de récurrence appliquée à l'orthogonal de e_1 montre que

$$\prod_{2 \leqslant i < j} (a_i, a_j)_p = \prod_{2 \leqslant i < j} (a'_i, a'_j)_p,$$

d'où le résultat. ◪

Nous écrirons donc $\epsilon(f)$ au lieu de $\epsilon(\mathcal{B})$. Passons maintenant à la représentation d'un élément de k par une forme quadratique.

Lemme 6 *Notons r le nombre d'éléments du $\mathbb{F}_2$-espace vectoriel k^*/k^{*2} (on a vu que $r = 2$ si $p \neq 2$ et $r = 3$ si $p = 2$).*

a) Soient $a \in k^*/k^{*2}$ et $\epsilon \in \{\pm 1\}$. Soit $H_a^\epsilon := \{x \in k^*/k^{*2},\ (x, a)_p = \epsilon\}$. Si $a = 1$, alors H_a^1 a 2^r éléments et $H_a^{-1} = \varnothing$. Si $a \neq 1$ alors H_a^ϵ a 2^{r-1} éléments.

b) Soient $a, a' \in k^*/k^{*2}$ et $\epsilon, \epsilon' \in \{\pm 1\}$; on suppose que H_a^ϵ et $H_a^{\epsilon'}$ sont non vides. Pour que $H_a^\epsilon \cap H_a^{\epsilon'} = \varnothing$, il faut et il suffit que $a = a'$ et $\epsilon = \epsilon'$.

Démonstration :
Montrons a). Le cas où $a = 1$ est trivial. Supposons $a \neq 1$. Le morphisme $b \mapsto (a, b)_p$ applique k^*/k^{*2} sur $\{\pm 1\}$, son noyau H_a^1 est donc un hyperplan de k^*/k^{*2} et a donc 2^{r-1} éléments ; son complémentaire H_a^{-1} a aussi 2^{r-1} éléments vu les valeurs possible de r. Montrons maintenant b). Compte tenu de a), si H_a^ϵ et $H_{a'}^{\epsilon'}$ sont non vides et disjoints alors ils ont nécessairement 2^{r-1} éléments chacun et sont complémentaires l'un de l'autre. Cela entraîne $H_a^1 = H_{a'}^1$, d'où $(x, a)_p = (x, a')_p$ pour tout $x \in k^*/k^{*2}$. Comme le symbole de Hilbert est non dégénéré, on en déduit $a = a'$, puis $\epsilon = \epsilon'$ évidement. La réciproque est triviale. ◪

Soit f une forme quadratique non dégénérée sur k^n. Notons $d = d(f)$ et $\epsilon = \epsilon(f)$. Nous omettrons l'indice p, correspondant au corps k, dans l'écriture des symboles de Hilbert

Théorème 11 *Pour que f représente 0, il faut et il suffit que l'une des conditions suivantes soit vérifiée :*

- *$n = 2$ et $d = -1$ (dans k^*/k^{*2}) ;*
- *$n = 3$ et $(-1, -d) = \epsilon$;*
- *$n = 4$ et, soit $d \neq 1$, soit $d = 1$ et $\epsilon = (-1, -1)$;*
- *$n \geqslant 5$.*

Démonstration :
En se plaçant dans une base orthogonale pour f on peut supposer que f est de la forme $f(X_1, \ldots, X_n) = a_1 X_1^2 + \cdots + a_n X_n^2$ avec $a_1, \ldots, a_n \in k^*$. Si $n = 1$ alors f ne représente pas 0 car f est supposée non dégénérée.

Supposons que $n = 2$. Alors f représente 0 si et seulement si $\frac{-a1}{a2}$ est un carré. Or, dans k^*/k^{*2}, on a $\frac{-a_1}{a_2} = -a_1a_2 = -d$, donc f représente 0 si et seulement si $-d = 1$ c'est-à-dire $d = -1$.

Supposons que $n = 3$. Alors f représente 0 si et seulement si la forme $-a_3 f$ représente 0, c'est-à-dire si et seulement si $(-a_3a_1, -a_3a_2) = 1$. En développant on obtient :

$$(-1,-1)(-1,a_1)(-1,a_2)(a_3,a_3)(a_1,a_2)(a_1,a_3)(a_2,a_3) = 1.$$

Mais d'après la proposition 10 on a $(a_3, a_3) = (-1, a_3)$. On réécrit alors la condition précédente sous la forme :

$$(-1,-1)(-1,a_1a_2a_3)(a_1,a_2)(a_1,a_3)(a_2,a_3) = 1,$$

ou encore $(-1,-d)\epsilon = 1$, c'est-à-dire $(-1,-d) = \epsilon$.

Supposons que $n = 4$. D'parès le corollaire 7, f représente 0 si et seulement si il existe $x \in k^*/k^{*2}$ qui est représenté par les formes

$$(X_1, X_2) \mapsto a_1X_1^2 + a_2X_2^2 \text{ et } (X_3, X_4) \mapsto -a_3X_3^2 - a_4X_4^2.$$

D'après le cas $n = 2$ du corollaire suivant (qui n'utilise pas le cas que nous somme en train de démontrer) un tel x est caractérisé par les conditions

$$(x, -a_1a_2) = (a_1, a_2) \text{ et } (x, -a_3a_4) = (-a_3, -a_4).$$

Soient $A := \{x \in k^*/k^{*2},\ (x, -a_1a_2) = (a_1, a_2)\}$ et $B := \{x \in k^*/k^{*2},\ (x, -a_3a_4) = (-a_3, -a_4)\}$. Pour que f ne représente pas 0, il faut et il suffit qu que $A \cap B = \varnothing$. Or A et B ne sont pas vides ($a_1 \in A$ et $-a_3 \in B$). D'après la partie b) du lemme 6, la relation $A \cap B = \varnothing$ équivaut donc à :

$$a_1a_2 = a_3a_4 \text{ et } (a_1, a_2) = -(-a_3, -a_4).$$

La première condition signifie que $d = 1$. Si elle est réalisée, on a $\epsilon = (a_1, a_2)(a_3, a_4)(a_3a_4, a_3a_4)$, et en utilisant la relation "$(x, x) = (-1, x)$" (proposition 10 4)) on en déduit :

$$\epsilon = (a_1, a_2)(a_3, a_4)(-1, a_3a_4) = (a_1, a_2)(-a_3, -a_4)(-1, -1).$$

On voit ainsi que la seconde condition s'écrit $\epsilon = -(-1, -1)$, d'où le résultat.

Supposon $n \geqslant 5$. On voit immédiatement qu'il suffit de traiter le cas $n = 5$. En utilisant le lemme 6 et le cas $n = 2$ du corollaire suivant, on voit qu'une forme de rang 2 représente au moins 2^{r-1} éléments de k^*/k^{*2}, et il en est a fortiori de même pour les formes de rang plus grand que 2. Comme $2^{r-1} \geqslant 2$, f représente au moins un éléments $a \in k^*/k^{*2}$ qui est distinct de d. D'après le corollaire 6 f est alors équivalente à $aX^2 \oplus g$ où $aX^2 : x \mapsto ax^2$ et g est une forme quadratique de rang 4. Le discriminant de g est égal à $d/a \neq 1$, donc, d'après le cas $n = 4$, la forme g représente 0. Il en est alors de même de f. ◲

Corollaire 8 *Soit $a \in k^*/k^{*2}$. Pour que f représente a, il faut et il suffit que l'une des conditions suivantes soit vérifiée :*

- *$n = 1$ et $a = d$;*
- *$n = 2$ et $(a, -d) = \epsilon$;*
- *$n = 3$ et, soit $a \neq -d$, soit $a = -d$ et $(-1, -d) = \epsilon$;*
- *$n \geqslant 4$.*

Démonstration :
Soit $a \in k^*/k^{*2}$ et considérons les formes sur k $aZ^2 : z \mapsto az^2$ et $f_a := f \ominus aZ^2$. D'après le corollaire 6, f_a représente 0 si et seulement si f représente a. Or on a immédiatement $d(f_a) = -ad$ et $\epsilon(f_a) = (-a, d)_p\epsilon$. On applique alors le théorème précédent à f_a. ◲

Chapitre 6

Théorème de Hasse-Minkowski.

Soit f une forme quadratique sur $\mathbb{Q}$. On note encore V la réunion de l'ensemble des nombres premiers et du symbole ∞. Pour tout $v \in V$, l'injection $\mathbb{Q} \to \mathbb{Q}_v$ (avec $\mathbb{Q}_\infty = \mathbb{R}$) permet de considérer f comme une forme quadratique (que nous noterons f_v) sur $\mathbb{Q}_v$.

Théorème 12 (Hasse-Minkowski) *Soit f une forme quadratique sur $\mathbb{Q}$ non dégénérée. Pour que f représente 0, il faut et il suffit que, pour tout $v \in V$, la forme f_v représente 0.*

La nécéssité est immédiate. Avant de démontrer la suffisance on indique quelques remarques et rappels.

Notons n le rang de f. Quitte à changer de base (en prenant une base orthogonale pour f) on peut supposer que f est de la forme

$$f(X_1, \ldots, X_n) = a_1 X_1^2 + \cdots + a_n X_n^2, \quad a_1, \ldots, a_n \in \mathbb{Q}^*.$$

On associe à f les invariants suivants :

- Le discriminant $d(f) \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ égal à $a_1 \ldots a_n$.

- Les invariants de f_v ($v \in V$) seront notés $d_v(f)$ et $\epsilon_v(f)$; $d_v(f)$ est l'image de $d(f)$ par l'injection $\mathbb{Q}^*/\mathbb{Q}^{*2} \to \mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$; on a

$$\epsilon_v(f) = \prod_{i<j} (a_i, a_j)_v.$$

  La formule du produit entraîne la relation

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

- La signature (r, s) de la forme quadratique réelle f_∞.

Démonstration :

Supposons que pour tout $v \in V$ la forme f_v représente 0, et montrons que f représente 0. On considère séparément les cas $n = 1, 2, 3, 4$, et $\geqslant 5$.

Le cas $n = 1$ est trivial : f représente 0 si, et seulement si f est identiquement nulle, et il en est de même pour f_∞.

Le cas $n = 2$. Quitte à remplacer f par $a_1 f$ on peut supposer $a_1 = 1$. On écrit $f(X_1, X_2) = X_1^2 - aX_2^2$. Comme f_∞ représente 0, le nombre a est strictement positif. Notons $\mathcal{P}$ l'ensemble des nombres premiers et écrivons a sous la forme $a = \prod_{p \in \mathcal{P}} p^{v_p(a)}$. Pour tout $p \in \mathcal{P}$, comme f_p représente 0, il existe $x, y \in \mathbb{Q}_p$ avec $y \neq 0$ tels que $x^2 - ay^2 = 0$, donc $a = (\frac{x}{y})^2$ est un carré dans $\mathbb{Q}_p$ et donc $v_p(a)$ est pair. Ainsi a est un carré dans $\mathbb{Q}$ et f représente bien 0.

Le cas $n = 3$. Quitte à remplacer f par $a_1 f$ on peut supposer $a_1 = 1$. On a $f(X_1, X_2, X_3) = X_1^2 - aX_2^2 - bX_3^2$. Quitte à multiplier a et b par des carrés, ce qui ne change pas les symboles de Hilbert par la proposition 10, on peut les supposer entiers sans facteurs carrés (c'est-à-dire que pour tout $p \in \mathcal{P}$ on a $v_p(a) \in \{0, 1\}$ et de même pour b). De plus, quitte à échanger les variables X_2 et X_3 on peut supposer $|a| \leqslant |b|$.

On raisonne alors par récurrence sur l'entier $m = |a| + |b| \geqslant 2$. Si $m = 2$, on a $f(X_1, X_2, X_3) = X_1^2 \pm X_2^2 \pm X_3^2$; le cas $X_1^2 + X_2^2 + X_3^2$ étant exclu car f_∞ représente 0, et dans les autres cas f représente bien 0 (il y a des solutions évidentes).

Soit $m > 2$, c'est-à-dire $|b| \geqslant 2$, supposons le résultat vrai pour tout $m' < m$ (c'est-à-dire que le théorème de Hasse-Minkowski est vrai pour toute forme quadratique équivalente à $(X_1, X_2, X_3) \mapsto X_1^2 - a'X_2^2 - b'X_3^2$ où $|a'| + |b'| < m$). Écrivons b sous la forme $b = \pm p_1 \dots p_k$ où les p_i, $i = 1, \dots, k$ sont des nombres premiers distincts. Soit $i \in \{1, \dots, k\}$ et notons $p = p_i$; nous allons voir que a est un carré modulo p. C'est immédiat si $a \equiv 0 \pmod{p}$. Sinon, a est une unité p-adique ; par hypothèse il existe $(z, x, y) \in \mathbb{Q}_p^3 / \{(0, 0, 0)\}$ tel que $z^2 - ax^2 - by^2 = 0$, de plus, par la proposition 8 on peut supposer $(z, x, y) \in \mathbb{Z}_p^3$ et que (z, x, y) est primitif. On a $z^2 - ax^2 \equiv 0 \pmod{p}$. Donc si $x \equiv 0 \pmod{p}$, il en est de même de z et alors p^2 divise by^2 donc p divise y contrairement au fait que (z, x, y) est primitif. On a donc $x \not\equiv 0 \pmod{p}$ et a est un carré modulo p ($a \equiv (\frac{z}{x})^2 \pmod{p}$). Comme, par le lemme chinois, $\mathbb{Z}/b\mathbb{Z} \simeq \prod_{i=1}^k \mathbb{Z}/p_i\mathbb{Z}$, on voit que a est un carré modulo $|b|$. Il existe donc des entiers t, b' tel que $t^2 = a + bb'$ et on peut choisir t tel que $|t^2| \leqslant |b| - 1$ (car $\{\bar{0}, \dots, |b| - 1\}$ est un système de représentant de $\mathbb{Z}/b\mathbb{Z}$) et donc tel que $|t| \leqslant \frac{|b|}{2}$. La formule $bb' = t^2 - a$ montre que bb' est une norme de l'extension $k(\sqrt{a})/k$, où $k = \mathbb{Q}$ ou $\mathbb{Q}_v$. On conclut, par la proposition 9 que f représente 0 dans k si et seulement s'il en est de même de f' où $f'(X_1, X_2, X_3) = X_1^2 - aX_2^2 - b'X_3^2$. En particulier f' représente 0 dans chacun des $\mathbb{Q}_v$. Mais on a :

$$|b'| = |\frac{t^2 - a}{b}| \leqslant \frac{|b|}{a} + 1 < |b| \quad \text{puisque } |b| \geqslant 2.$$

Écrivons $b' = b''u^2$ avec b'', u entiers et b'' sans facteurs carrés ; on a $|b''| \leqslant |b'| < |b|$. L'hypothèse de récurrence s'applique donc à f'' où $f''(X_1, X_2, X_3) = X_1^2 - aX_2^2 - b''X_3^2$. Ainsi f'' représente 0, et il en est de même de f' puis de f. Ceci achève la récurrence et démontre le cas $n = 3$.

Le cas $n = 4$. On a :

$$f(X_1, \dots, X_4) = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2).$$

Soit $v \in V$. Puisque f_v représente 0, le corollaire 7 montre qu'il existe $x_v \in \mathbb{Q}_v^*$ qui est représenté à la fois par $aX_1^2 + bX_2^2$ et par $cX_3^2 + dX_4^2$; d'après le corollaire 8 (qui s'applique également à $\mathbb{Q}_\infty = \mathbb{R}$), cela revient à dire que l'on a :

$$(x_v, -ab)_v = (a, b)_v \quad \text{et} \quad (x_v, -cd)_v = (c, d)_v.$$

Comme $\prod_{v \in V} (a, b)_v = \prod_{v \in V} (c, d)_v = 1$, on peut appliquer le théorème 8 et l'on conclut qu'il existe $x \in \mathbb{Q}^*$ tel que :

$$(x, -ab)_v = (a, b)_v \quad \text{et} \quad (x, -cd)_v = (c, d)_v \text{ pour tout } v \in V.$$

La forme $aX_1^2 + bX_3^2 - xZ^2$ représente alors 0 dans chacun des $\mathbb{Q}_v$ donc dans $\mathbb{Q}$ d'après le cas $n = 3$ démontré précédement. Ainsi x est représenté dans $\mathbb{Q}$ par $aX_1^2 + bX_2^2$, et le même argument s'applique à $cX_3^2 + dX_4^2$, ce qui montre que f représente 0.

Le cas $n \geqslant 5$. On raisonne par récurrence sur n. Soit $n \geqslant 5$; on suppose que le théorème de Hasse-Minkowski est vrai pour toute les formes quadratiques en $n - 1$ variables ou moins. On écrit f sous la forme $f = h - g$ avec $h = a_1X_1^2 + a_2X_2^2$ et $g = -(a_3X_3^2 + \dots + a_nX_n^2)$.

Soit S la partie de V formée de $\infty, 2$ et des nombres premiers p tels que $v_p(a_i) \neq 0$ pour au moins un $i \geqslant 3$; c'est un ensemble fini puisqu'il n'y a qu'un nombre fini de a_i. Soit $v \in S$. Puisque f_v représente 0,

il existe $a_v \in \mathbb{Q}^*$ qui est représenté dans $\mathbb{Q}_v$ par h et par g. Il existe donc $x_i^v \in \mathbb{Q}_v,\ i = 1, \ldots, n$, tels que : $h(x_1^v, x_2^v) = a_v = g(x_3^v, \ldots, x_n^v)$. Mais les carrés de $\mathbb{Q}_v^*$ forment un ensemble ouvert de $\mathbb{Q}_v^*$ (théorème 4), donc par le lemme d'aproximation 4 il existe $x_1, x_2 \in \mathbb{Q}$ tels que ,si $a = h(x_1, x_2)$, on ait $a/a_v \in \mathbb{Q} - v^{*2}$ pour tout $v \in S$. Considérons maintenant la forme $f_1 := k \ominus g$, où $k : z \mapsto az^2$. Si $v \in S$ alors g représente a_v dans $\mathbb{Q}_v$, il existe $(y_3, \ldots, y_n) \in \mathbb{Q}_v^{n-3}$ tel que $g(y_3, \ldots, y_n) = a_v$, mais $a/a_v \in \mathbb{Q}_v^{*2}$ donc il existe $w \in \mathbb{Q}_v^*$ tel que $w^2 = a/a_v$, donc $g(y_3 w, \ldots, y_n w) = a$; on en conclut que f_1 représente 0 dans $\mathbb{Q}_v$. Si $v \notin S$ alors les coefficients $-a_3, \ldots, -a_n$ de g sont des unités v-adiques ; il en est donc de même de $d_v(g)$, de plus, comme $v \neq 2$ on a $\epsilon_v(g) = 1$ (par le théorème 5). Comme le rang de g vaut au moins 3, le théorème 11 montre que g représente 0. Dans tous les cas on voit que f_1 représente 0 dans $\mathbb{Q}_v$; comme le rang de f_1 est $n-1$, l'hypothèse de récurrence indique que f_1 représente 0 dans $\mathbb{Q}$, c'est-à-dire que g représente a dans $\mathbb{Q}$. Comme h représente a dans $\mathbb{Q}$ on obtient bien que f représente 0 sur $\mathbb{Q}$. ◲

Corollaire 9 *Soit f une forme quadratique sur $\mathbb{Q}$ non dégénérée, et soit $a \in \mathbb{Q}^*$. Pour que f représente a (dans $\mathbb{Q}$), il faut et il suffit qu'il en soit ainsi dans chacun des $\mathbb{Q}_v$, $v \in V$.*

Démonstration :
Cela résulte immédiatement du théorème de Hasse-Minkowski, appliqué à la forme $aZ^2 - f$.

Corollaire 10 *Une forme quadratique sur $\mathbb{Q}$ non dégénérée de rang $n \geqslant 5$ représente 0 si et seulement si elle est indéfinie (c'est-à-dire si f_∞ représente 0).*

Démonstration :
En effet, d'après le théorème 11, une telle forme représente 0 dans chacun des $\mathbb{Q}_p$ et on applique le théorème de Hasse-Minkowski.

Terminons cette partie par une application. Soient $n, p \in N^*$. On dit que n est somme de p carrés s'il existe des entiers $n_1, \ldots, n_p$ tels que $n = n_1^2 + \cdots + n_p^2$. Nous allons déterminer les entiers qui sont somme de trois ou quatre carrés.

Lemme 7 *Soit $a \in \mathbb{Q}^*$. Pour que a soit représenté sur $\mathbb{Q}$ par la forme $f : (X_1, X_2, X_3) \mapsto X_1^2 + X_2^2 + X_3^2$, il faut et il suffit que a soit strictement positif et que $-a$ ne soit pas un carré dans $\mathbb{Q}_2$.*

Démonstration :
D'après le corollaire 9, il faut exprimer le fait que a est représenté sur $\mathbb{Q}_v$ par f_v pour tout $v \in V$. Le cas de $\mathbb{R}$ donne immédiatement la condition "$a > 0$". Soit p un nombre premier, les invariants locaux $d_p(f)$ et $\epsilon_p(f)$ sont égaux à 1. Si $p \neq 2$ alors on a :

$$(-1, d_p(f))_p = (-1, -1)_p = 1 = \epsilon_p(f);$$

le corollaire 8 montre alors que a est représenté par f_p sur $\mathbb{Q}_p$. Si $p = 2$ on a $(-1, -d_2(f))_2 = -1 \neq \epsilon_2(f)$ et le corollaire 8 montre que a est représenté par f_2 si et seulement si a est différent de -1 dans $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$, c'est-à-dire si $-a$ n'est pas un carré de $\mathbb{Q}_2$. ◲

Lemme 8 (Davenport-Cassels) *Soit $p \in N^*$ et soit $A = (a_{i,j})_{1 \leqslant i,j \leqslant p}$ une matrice symétrique définie positive à coefficients entiers. On note f la forme quadratique associée à A. On suppose que pour tout $x = (x_1, \ldots, x_p) \in \mathbb{Q}^p$, il existe $y \in \mathbb{Z}^p$ tel que $f(x - y) < 1$. Alors, si n est représenté par f sur $\mathbb{Q}$, n est aussi représenté par f sur $\mathbb{Z}$.*

Démonstration :
Si $x = (x_1, \ldots, x_p)$ et $y = (y_1, \ldots, y_p)$ sont deux éléments de $\mathbb{Q}_p$, on note $x.y := \sum 1 \leqslant i, j \leqslant p a_{i,j} x_i y_j$ leur produit scalaire. On a $x.x = f(x)$. Soit n un entier représenté par f sur $\mathbb{Q}$. Il existe $t \in \mathbb{N}^*$ tel que

$t^2n = f(x) = x.x$ avec $x \in \mathbb{Z}^p$. Toute partie non vide de $\mathbb{N}^*$ admettant un minimum, on choisir t et x de telle sorte que t soit minimal ; nous faisons donc cette hypothèse, nous allons montrer que $t = 1$, ce qui prouvera le lemme. D'après l'hypothèse du lemme, il existe $y \in \mathbb{Z}^p$ tel que $\frac{x}{t} = y + z$, avec $z.z < 1$. Si $z.z = 0$ alors $z = 0$ et donc $\frac{x}{t}$ est a composantes entières. Vu la minimalité de t, cela entraîne $t = 1$. Supposons que l'on ait $z.z \neq 0$, et posons :

$$a = y.y - n \quad b = 2(nt - x.y) \quad t' = at + b \quad x' = ax + by.$$

On a $a, b, t' \in \mathbb{Z}$ et :

$$\begin{aligned} x'.x' = a^2x.x + 2abx.y + b^2y.y &= a^2t^2n + ab(2nt - b) + b^2(n + a) \\ &= n(a^2t^2 + 2abt + b^2) \\ &= t'^2n. \end{aligned}$$

D'autre part :

$$\begin{aligned} tt' = at^2 + bt = t^2y.y - nt^2 + 2nt^2 - 2tx.y &= t^2y.y - 2tx.y + x.x \\ &= (ty - x).(ty - x) \\ &= t^2z.z, \end{aligned}$$

d'où $t' = tz.z$. Mais $0 < z.z < 1$ donc $0 < t' < t$, ce qui contredit la minimalité de t. ◪

Théorème 13 *Pour qu'un entier strictement positif n soit somme de trois carrés, il faut et il suffit qu'il ne soit pas de la forme $4^a(8b - 1)$, avec $a, b \in \mathbb{Z}$.*

Démonstration :
Par le théorème 3, la condition «n est de la forme $4^a(8b - 1)$» équivaut à dire que $-n$ est un carré dans $\mathbb{Q}_2^*$. Notons f la forme quadratique sur $\mathbb{Q}$ définie par $f(X_1, X_2, X_3) = X_1^2 + X_2^2 + X_3^2$. Alors,par le lemme 7, la forme f représente n sur $\mathbb{Q}$. Mais f est évidement définie positive, de matrice a coefficients entiers, de plus, pour tout $x = (x_1, x_2, x_3) \in \mathbb{Q}^3$ on peut choisir $y = (y_1, y_2, y_3) \in \mathbb{Z}^3$ tel que $|x_i - y_i| \leqslant 1/2$ $(i = 1, 2, 3)$ et on a $f(x - y) \leqslant 3/4 < 1$. On conclut alors par le lemme 8 que n est somme de trois carrés. ◪

Théorème 14 *Tout entier positif est somme de quatre carrés.*

Démonstration :
Soit n un entier strictement positif (0 est bien somme de quatre carrés). On écrit n sous la forme $n = 4^am$ où m n'est pas divisible par 4. Si m est congru a 1,2,3,5 ou 6 modulo 8 alors m est somme de trois carrés par le théorème précédent, et un nombre somme de trois carrés est évidement aussi somme de quatre carrés. Sinon, on a $m \equiv -1 \pmod 8$, et $m - 1$ est somme de trois carrés donc, comme $1 = 1^2$, m est somme de quatre carrés et n aussi (car $4^a = 2^{2a}$ est un carré). ◪

Chapitre 7

Compléments.

Dans ce chapitre nous aborderons d'autres équations diophantiennes que celles définies par un polynôme homogène de degré 2, notamment l'équation $3X^3 + 4Y^3 + 5Z^3 = 0$ qui montre que le théorème de Hasse-Minkowski ne se généralise pas aux polynômes homogènes de degré 3, ainsi que les systèmes d'équations diophantiennes de degré 1 pour lesquels il existe une méthode de résolution systématique.

7.1 Contre-exemples au principe «local-global».

Si (E) désigne une équation diophantienne dont on cherche des solutions rationnelles, on dit que le principe «local-global» s'applique à (E) si l'affirmation «Si (E) admet une solution non nulle sur $\mathbb{R}$ et sur $\mathbb{Q}_p$ pour tout nombre premier p, alors (E) admet une solution non nulle sur $\mathbb{Q}$.» est vraie. Le théorème de Hasse-Minkowski nous donne un cas où le principe «local-global» s'applique, et dans cette partie nous allons donner deux exemples où ce principe ne s'applique pas. Le premier exemple est élémentaire, quand au deuxième il montre que le théorème de Hasse-Minkowski ne se généralise pas aux polyômes homogènes de degré 3.

Proposition 14 *L'équation*

$$(x^2 - 2)(x^2 - 17)(x^2 - 34) = 0 \tag{7.1}$$

admet une solution (non nulle) sur $\mathbb{R}$ et sur $\mathbb{Q}_p$ pour tout nombre premier p, mais elle n'a pas de solution sur $\mathbb{Q}$.

Démonstration :
Il est évident que (7.1) a une solution réelle mais pas de solution rationnelle. Considérons maintenant un nombre premier p et montreons qu'au moins l'un des nombres 2,17,34 est un carré dans $\mathbb{Q}_p$, ce qui montrera que (7.1) possède une solution dans $\mathbb{Q}_p$. Pour cela on utilise les théorèmes 2 et 3. Comme $17 = 1 + 2^4 \equiv 1 \pmod 8$, 17 est un carré dans $\mathbb{Q}_2$. Comme $2 \equiv 6^2 \pmod{17}$, 2 est un carré dans $\mathbb{Q}_{17}$. On suppose alors $p \neq 2, 17$. Comme $(\frac{2}{p})(\frac{17}{p}) = (\frac{34}{p})$, on en déduit que si 2 et 17 ne sont pas des carrés dans $\mathbb{Q}_p$ alors 34 est un carré dans $\mathbb{Q}_p$, donc (7.1) a bien une solution dans $\mathbb{Q}_p$.

Le contre-exemple suivant, dû à Selmer, est beaucoup plus difficile et nous n'en donnerons pas une preuve détaillée. On trouvera dans le livre de Henri Cohen [2] une étude approfondie des équations diophantiennes de la forme $ax^p + by^p + cz^p = 0$.

Théorème 15 *L'équation*

$$3X^3 + 4Y^3 + 5Z^3 = 0 \tag{7.2}$$

admet une solution non nulle dans $\mathbb{R}^3$ et dans $\mathbb{Q}_p^3$ pour tout nombre premier p, mais n'admet pas de solution non nulle dans $\mathbb{Q}^3$.

Démonstration :
Montrons que l'équation (7.2) admet localement des solutions non nulles. Il y a évidement des solutions réelles, par exemple $(1, (\frac{3}{4})^{\frac{1}{3}}, 0)$. Soit p un nombre premier ; nous allons montrer que (7.2) admet une solution non nulle sur $\mathbb{Z}_p$ à l'aide du lemme de Hensel 1. Si $p = 3$ alors l'équation $4y^3 - 5 = 0$ a une solution modulo $3^3 = 27$ (il s'agit de 2) et comme $v_3(3 \times 4 \times 2^2) = 1$ avec $2 \times 1 < 3$ le lemme de Hensel prouve qu'il existe $y_0 \in \mathbb{Z}_3$ tel que $4y_0^3 - 5 = 0$. Alors $(0, y_0, -1)$ est une solution de (7.2) dans $\mathbb{Z}_3$. Si $p = 5$ alors 2 est solution modulo 5 de l'équation $4y^3 + 3 = 0$ donc par le lemme de Hensel il existe $y_0 \in \mathbb{Z}_5$ tel que $4y_0^3 + 3 = 0$ et $(1, y_0, 0)$ est solution de (7.2) dans $\mathbb{Z}_5$. On suppose maintenant que $p \notin \{3, 5\}$. S'il existe $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $3 = a^3$ alors $\frac{1}{a}$ est une solution modulo p de $3x^3 - 1 = 0$, donc il existe $x_0 \in \mathbb{Z}_p$ tel que $3x_0^3 - 1 = 0$ et alors $(x_0, 1, -1)$ est une solution de (7.2) dans $\mathbb{Z}_p$. Si 3 n'est pas un cube dans $(\mathbb{Z}/p\mathbb{Z})^\times$, alors le groupe des cubes de $(\mathbb{Z}/p\mathbb{Z})^\times$, que nous noterons $(\mathbb{Z}/p\mathbb{Z})^{\times 3}$, est d'indice 3, et $\{1, 3, 9\}$ est un système de représentants de $(\mathbb{Z}/p\mathbb{Z})^\times/(\mathbb{Z}/p\mathbb{Z})^{\times 3}$. On considère alors les trois cas suivant :

- Si 5 est un cube, alors $5z^3 - 1 = 0$ a une solution modulo p donc il existe $z_0 \in \mathbb{Z}_p$ tel que $5z_0^3 - 1 = 0$ et $(-1, 1, z_0)$ est une solution de l'équation (7.2) dans $\mathbb{Z}_p$.

- Si $\frac{5}{3}$ est un cube, alors $5z^3 - 3 = 0$ a une solution modulo p donc il existe $z_0 \in \mathbb{Z}_p$ tel que $5z_0^3 - 3 = 0$ et $(-1, 0, z_0)$ est une solution de l'équation (7.2) dans $\mathbb{Z}_p$.

- Si $\frac{5}{9}$ est un cube, alors $t^3 - 15 = 0$ a une solution modulo p donc il existe $t_0 \in \mathbb{Z}_p$ tel que $t_0^3 - 15 = 0$ et $(3t_0, 5, -7))$ est une solution de l'équation (7.2) dans $\mathbb{Z}_p$.

Indiquons maintenant comment montrer que (7.2) n'a pas de solution rationnelle non nulle. En écrivant (7.2) sous la forme $(2y)^3 + 6x^3 = 10(-z)^3$ on remarque qu'il suffit de montrer que l'équation $x^3 + 6y^3 = 10z^3$ n'a pas de solution non nulle sur $\mathbb{Q}$; supposons que (a, b, c) soit une telle solution, quitte à éliminer les dénominateurs on peut supposer que a, b et c sont entiers et premiers entre eux dans leur ensemble. Alors $abc \neq 0$ et on a $(a + b\sqrt[3]{6})(a^2 - ab\sqrt[3]{6} + b^2\sqrt[3]{36}) = 10c^3$. Il convient donc d'étudier la structure de $O_K := \mathbb{Z}[\sqrt[3]{6}]$, pour montrer que cette égalité est impossible. On procède de la manière suivante.

Étape 1 : On montre que $\mathbb{Z}[\sqrt[3]{6}]$ est l'anneau des entiers du corps de nombres $K := \mathbb{Q}[\sqrt[3]{6}]$, et que son discriminant est $-2^2 \times 3^5$.

Étape 2 : On montre que O_K est principal. Au cours de cette étape on est ammené à factoriser (p) pour $p \in \{2, 3, 5, 7\}$: on écrit $(2) = p_2^3$, $(3) = p_3^3$, $(5) = p_5 p_{25}$ et $(7) = p_7 p_7' p_7''$.

Étape 3 : On montre que $(a + b\sqrt[3]{6}, a^2 - ab\sqrt[3]{6} + b^2\sqrt[3]{36}) = p_2$.

Étape 4 : On montre que $(a + b\sqrt[3]{6})$ est inclu dans p_5 mais pas dans (5).

Étape 5 : On a $(a + b\sqrt[3]{6})(a^2 - ab\sqrt[3]{6} + b^2\sqrt[3]{36}) = p_2^3 p_5 p_{25} c^3$ et à l'aide des étapes 3 et 4 on en déduit qu'il existe $\alpha \in O_K$ et $u \in O_K^\times$ te que $a + b\sqrt[3]{6} = (2 - \sqrt[3]{6})(1 + \sqrt[3]{6})\alpha^3 u$.

Étape 6 : En utilisant le théorème des unités de Dirichlet on montre que l'on peut supposer que $u = (\frac{(2-\sqrt[3]{6})^3}{2})^k$ avec $k \in \{0, 1, 2\}$.

Étape 7 : En multipliant par 2^k la relation obtenue à l'étape 5 on obtient $2^k(a + b\sqrt[3]{6}) = (2 - \sqrt[3]{6})(1 - \sqrt[3]{6})\beta^3$, où $\beta = (2 - \sqrt[3]{6})^k\alpha$. On écrit alors β sous la forme $A + B\sqrt[3]{6} + C\sqrt[3]{36}$ avec $A, B, C \in \mathbb{Z}$, et en comparant les coefficients devant $\sqrt[3]{36}$ on obtient :

$$0 = A^3 + 6B^3 + 36C^3 + 36ABC - 9(A^2B + 6B^2C + 6C^2A) + 6(AB^2 + 6BC^2 + CA^2).$$

Enfin, on en en déduit que $A = B = C = 0$ et donc que $a = b = 0$, ce qui est absurde.

7.2 Les équations diophantiennes homogènes de degré 1.

7.2.1 Une équation.

Soient $k \in \mathbb{N}^*$, $(a_1, \ldots, a_k) \in \mathbb{Z}^k \backslash (0, \ldots, 0)$, $b \in \mathbb{Z}$ et considérons l'équation diophantienne :

$$a_1 x_1 + \cdots + a_k x_k = b. \tag{7.3}$$

(7.4)

Proposition 15 *Soient $a_1, \ldots, a_k, d$ des éléments d'un anneau principal A. Si d est un* pgcd *de $a_1, \ldots, a_k$ alors il existe $(u_1, \ldots, u_k) \in A^k$ tel que $d = a_1 u_1 + \cdots + a_k u_k$.*

Démonstration :
Si d est un pgcd de $a_1, \ldots, a_k$ alors il appartient à $a_1 A + \cdots + a_k A$, d'où l'existence de $u_1, \ldots, u_k$. Réciproquement, supposons que $d = a_1 u_1 + \cdots + a_k u_k$. Soit d_0 un pgcd de $a_1, \ldots, a_k$. On a $d \in a_1 A + \cdots + a_k A = d_0 A$ et donc d_0 divise d. De plus d est un diviseur commun de $a_1, \ldots, a_k$ donc un diviseur de d_0. Finalement d et d_0 sont associés donc d est un pgcd de $a_1, \ldots, a_k$.

Corollaire 11 (théorème de Bézout) *Pour que des éléments $a_1, \ldots, a_k$ d'un anneau principal A soient premiers entre eux dans leur ensemble, il faut et il suffit qu'il existe $(u_1, \ldots, u_k) \in A^k$ tel que $1 = a_1 u_1 + \cdots + a_k u_k$.*

Démonstration :
On applique la proposition précédente avec $d = 1$ qui divise $a_1, \ldots, a_k$.

Proposition 16 *Une condition nécéssaire est suffisante pour que* (7.3) *admette au moins une solution est que* $\text{pgcd}(a_1, \ldots, a_k)$ *divise b.*

Démonstration :
Notons d ce pgcd et $a_i =: d a_i'$ pour $i = 1, \ldots, n$. Si on a une solution $(x_1, \ldots, x_n)$ alors $d \sum_{i=1}^n a_i' x_i = b$ donc d divise b. Réciproquement si d divise b on note $b =: db'$ et on peut écrire (7.3) sous la forme $\sum_{i=1}^n a_i' x_i = b'$. Or $\text{pgcd}(a_1', \ldots, a_n') = 1$ donc par le théorème de Bézout il existe $(u_1, \ldots, u_n) \in \mathbb{Z}^n$ tel que $\sum_{i=1}^n a_i' u_i = 1$, d'où $\sum_{i=1}^n a_i' b' u_i = b'$ qui donne la solution $(b'u_1, \ldots, b'u_n)$.

Proposition 17 *On considère l'équation $ax + by = c$ où $(a, b, c) \in \mathbb{Z}^3$ et* $\text{pgcd}(a, b) = 1$. *Soient (x_0, y_0) une solution de l'équation, $a' = \dfrac{a}{d}$ et $b' = \dfrac{b}{d}$. L'ensemble des solutions de cette équation est $\{(x_0 - kb, y_0 + ka), k \in \mathbb{Z}\}$.*

Démonstration :
Soit (x, y) une solution de l'équation. On a $ax + by = c$ et $ax_0 + by_0 = c$ donc par soustraction $a(x - x_0) + b(y - y_0) = 0$ or a est premier avec b par hypothèse donc a divise $(y - y_0)$: il existe $k \in \mathbb{Z}$ tel que $y - y_0 = ka$. On a alors $a(x - x_0) + bka = 0$ donc $x = x_0 - kb$. Réciproquement, pour tout $k \in \mathbb{Z}$, $(x_0 - kb, y_0 + ka)$ est bien solution de l'équation.

Dans le cas à deux variables admettant une solution on peut toujours trouver une solution par l'algorithme d'Euclide étendu.

Exemple :
L'équation $56x + 15y = 1$ admet pour solution particulière $(-4, 15)$ et l'ensemble des solutions de cette équation est $\{(-4 - 15k, 15 + 56k), k \in \mathbb{Z}\}$.

On peut généraliser la méthode exposée dans la démonstration de la proposition 17.

Exemple :
On considère l'équation $20x + 15y + 45z = 175$. On commence par réduire cette équation sous la forme équivalente (E) $4x + 3y + 9z = 35$, avec cette fois-ci $\text{pgcd}(4, 3, 9) = 1$.

On remarque que $(8, 1, 0)$ est solution de (E), et on considère une solution (x, y, z) de (E). Par soustraction de ces deux solutions on obtient $4(x - 8) + 3(y - 1) + 9z = 0$, or 3 est premier avec 4 donc 3 divise $x - 8$; on écrit $x - 8 = 3\alpha$. On obtient alors $y = 1 - 4\alpha - 3z$. Réciproquement on vérifie que pour tout $(\alpha, z) \in \mathbb{Z}^2$ $(3\alpha + 8, 1 - 4\alpha - 3z, z)$ est solution de (E).

7.2.2 Systèmes d'équations linéaires

Dans cette partie on considère deux entiers strictement positifs n et m, une matrice $M \in \mathcal{M}_{n,m}(A)$ où A est un anneau principal, un vecteur $B \in \mathcal{M}_{n,1}$ et on cherche $X \in \mathcal{M}_{m,1}$ vérifiant :

$$MX = B \tag{7.5}$$
$$\tag{7.6}$$

On commence par un théorème de réduction.

Théorème 16 (Réduction de Smith) *Il existe deux matrices inversibles $P \in GL_n(A), Q \in GL_m(A)$ et une matrice $D = (d_{i,j})_{i,j} \in \mathcal{M}_{n,m}(A)$ quasi-diagonale (c'est-à-dire $d_{i,j} = 0$ pour $i \neq j$), telles que $M = PDQ$ et $d_{i,i}$ divise $d_{i+1,i+1}$ pour tout $i \in [\![1, \min(n, m)]\!]$.*
De plus, si $M = P'D'Q'$ est une autre décomposition de cette nature alors pour tout $i \in [\![1, \min(n, m)]\!]$ les scalaires $d_{i,i}$ et $d'_{i,i}$ sont associés.

Démonstration :
On commence par la partie «unicité». Notons $r = \min(n, m)$ et pour $k \leqslant r$ notons $D_k(M)$ le pgcd des mineurs d'ordre k de la matrice M. Par la formule de Binet-Cauchy $D_k(M) = D_k(D) = D_k(D')$ or $D_k(D) = d_{1,1} \dots d_{k,k}$ donc $d_{1,1} \dots d_{k,k} = u_k d'_{1,1} \dots d'_{k,k}$ avec $u_k \in A^*$ (et ce, pour tout $k \in [\![1, r]\!]$). Donc $d_{1,1}$ et $d'_{1,1}$ sont associés. Comme A est intègre, on a aussi $d'_{k,k} = u_k^{-1} u_{k-1} d_{k,k}$, donc $d_{k,k}$et $d'_{k,k}$ sont associés.

Passons maintenant à la partie «existence». Ce qui précède montre que les $d_{j,j}$ sont déterminés par les égalités $d_{1,1} \dots d_{j,j} = D_j(M)$. En particulier $d_{1,1}$ est le pgcd des coefficients de M. La première étape consiste donc à trouver une matrice $M' = (m'_{i,j})_{i,j}$ équivalente à M telle que $m'_{1,1}$ soit égale à ce pgcd.

On commence par construire une suite de matrices équivalentes $M^{(p)}$, $p \in \mathbb{N}$, avec $M^{(0)} = M$ et telles que $m_{1,1}^{(p)}$ divise $m_{1,1}^{(p-1)}$. Pour passer de $N = (n_{i,j})_{i,j} := M^{(p-1)}$ à $M^{(p)}$ il y a quatre cas :

- 1) si $n_{1,1}$ divise $n_{1,1}, \dots, n_{1,j-1}$ mais ne divise pas $n_{1,j}$. Alors $d := \text{pgcd}(n_{1,1}, n_{1,j})$ s'écrit $d = un_{1,1} + vn_{1,j}$ (dans l'anneau principal A). Notons $w = -\dfrac{n_{j,1}}{d}$ et $z = \dfrac{n_{1,1}}{d}$ et définissons une matrice $Q = (q_{i,j})_{i,j} \in GL_m(A)$ par :
  $q_{k,l} = \delta_k^l$, sauf si $\{k, l\} \cup \{1, j\}$;
  $q_{1,1} = u, q_{j,1} = v, q_{1,j} = w, q_{j,j} = z$.
  Alors $M^{(p)} := M^{(p-1)}Q$ convient, car $m_{1,1}^{(p)} = d$ divise $n_{1,1} = m_{1,1}^{(p-1)}$.

- 2) si $n_{1,1}$ divise tous les $n_{1,j}$ ainsi que $n_{1,1}, \dots, n_{i-1,1}$ mais ne divise pas $n_{i,1}$. Ce cas est symétrique au précédent, une multiplication à droite par $P \in GL_m(A)$ fournit $M^{(p)}$, avec $m_{1,1}^{(p)} = \text{pgcd}(n_{1,1}, n_{i,1})$ divise $m_{1,1}^{(p-1)}$.

– 3) si $n_{1,1}$ divise tous les $n_{1,j}$ et tous les $n_{i,1}$ mais ne divise pas un $n_{i,j}$ avec $i,j \geqslant 2$. Alors $n_{i,1} = an_{1,1}$. Définissons une matrice $P = (p_{i,j})_{i,j} \in GL_n(A)$ par :
-$p_{k,l} = \delta_k^l$, sauf si $\{k,l\} \cup \{i,1\}$;
-$p_{1,1} = a+1, p_{i,1} = 1, p_{1,i} = -1, p_{i,i} = 0$.
Posant alors $N' = PN$, on a $n'_{1,1} = n_{1,1}$ et $n'_{1,j} = (a+1)n_{1,j} - n_{i,j}$. Nous sommes donc ramenés au premier cas, et il existe une matrice équivalente $M^{(p)}$, avec $m_{1,1}^{(p)} = \text{pgcd}(n'_{1,1}, n'_{1,j}) = \text{pgcd}(n_{1,1}, n_{i,j}$ qui divise $n_{1,1} = m_{1,1}^{(p-1)}$.

– 4) si $n_{1,1}$ divise tous les coefficients de la matrice N. Dans ce cas on pose $M^{(p)} := M^{(p-1)}$.

Il est essentiel de noter que, dans les trois premiers cas, $m_{1,1}^{(p)}$, qui divise $m_{1,1}^{(p-1)}$, ne lui est pas associé.
Comme A est principal, il est noethérien et donc les éléments de la suite $\left(m_{1,1}^{(p)}\right)_{p\geqslant 0}$ sont tous associés à partir d'un certain rang q. On est alors dans le dernier cas : $m_{1,1}^{(q)}$ divise tous les $m_{i,j}^{(q)}$. On a $m_{i,1}^{(q)} = a_i m_{1,1}^{(q)}$ et $m_{1,j}^{(q)} = b_j m_{1,1}^{(q)}$. Soit alors $P = (p_{i,j})_{i,j} \in GL_n(A)$ et $Q = (q_{i,j})_{i,j} \in GL_m(A)$ les matrices définies par :
$p_{i,i} = 1, p_{i,1} = -a_i$ si $i \geqslant 2$, $p_{i,j} = 0$ sinon ;
$q_{j,j} = 1, q_{1,j} = -b_j$ si $j \geqslant 2$, $q_{i,j} = 0$ sinon.
La matrice $M' := PM^{(q)}Q$ est équivalente à $M^{(q)}$ donc à M. Elle est de la forme :

$$M' = \begin{pmatrix} m & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & M'' & \\ 0 & & & \end{pmatrix}$$

où m divise tous les coefficients de M''.
On peut alors montrer le théorème par récurrence sur $r = \min(n,m)$.
L'analyse précédente montre que le résultat est vrai pour $r = 1$.
Si $r \geqslant 2$ et si le résultat est vrai à l'ordre $r-1$ alors on applique l'hypothèse de récurrence au facteur $M'' \in \mathcal{M}_{(n-1)\times(m-1)}$ de la réduction ci-dessus : il existe $P'' \in GL_{n-1}(A)$ et $Q'' \in GL_{m-1}(A)$ telles que $P''M''Q''$ soit quasi-diagonale.
On pose alors $P' = \text{diag}(1, P'')$ et $Q' = \text{diag}(1, Q'')$ qui sont inversibles et on obtient une matrice quasi-diagonale $P'M'Q'$ équivalente à M' donc à M. Ceci achève la récurrence. ◻

Remarque 2 *Le plus grand entier i tel que $d_{i,i} \neq 0$ est le rang de M.*

Corollaire 12 *On considère le système (7.5) dans l'anneau $\mathbb{Z}$. Soit $(P,Q) \in GL_n(\mathbb{Z}) \times GL_m(\mathbb{Z})$ et $D \in \mathcal{M}_{n\times m}(\mathbb{Z})$ comme dans le théorème précédent. Notons $(b'_1, \dots, b'_n)^t = P^{-1}B \in \mathbb{Z}^n$. Alors le système $(*)$ n'a pas de solution si $b'_i \neq 0$ pour $i \geqslant r+1$ ($r = rg(A)$) et dans le cas contraire l'ensemble des solutions est :*

$$\{Q^{-1}(\frac{b'_1}{d_1}, \dots, \frac{b'_r}{d_r}, x_{r+1}, \dots, x_m)^t; (x_{r+1}, \dots, x_m) \in \mathbb{Z}^{m-r}\}.$$

Démonstration :
On note $M = PDQ$ et si X est une solution de (7.5) alors on a $P^{-1}A'Q^{-1}X = B$ puis on multiplie à gauche par $\text{diag}(d_{1,1}, \dots, d_{r,r}, 0, \dots, 0)P$. On remarque alors que l'on obtient bien le résultat voulu.

Pour obtenir P^{-1} et Q^{-1}, on effectue sur la matrice M des opérations élémentaires du type :
– échanger deux lignes ou deux colonnes ;
– ajouter à une ligne (resp. une colonne) a fois une autre ligne (resp. colonne), où $a \in \mathbb{Z}$.

On effectue ces opérations sur les lignes (resp. colonnes) dans le même ordre sur I_n (resp. I_m) pour obtenir la matrice P^{-1} (resp. Q^{-1}).

Exemple :
L'ensemble des solutions de $3x - 5y - 4z = 0$ est $\{ke_1 + le_2; (k,l) \in \mathbb{Z}^2\}$ où $e_1 = (-5,-3,0)$ et $e_2 = (8,4,1)$.
En effet, on a :

$$\begin{pmatrix} 3 & -5 & -4 \end{pmatrix} \to I_3$$

$$\begin{pmatrix} 3 & 1 & -4 \end{pmatrix} (C_2 \leftarrow C_2 + 2C_1) \to \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 3 & -4 \end{pmatrix} (C_1 \leftrightarrow C_2) \to \begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \end{pmatrix} (C_2 \leftarrow C_2 - 3C_1 et C_3 \leftarrow C_3 + 4C_1) \to \begin{pmatrix} 2 & -5 & 8 \\ 1 & -3 & 4 \\ 0 & 0 & 1 \end{pmatrix} = Q^{-1}$$

Exemple :
L'ensemble des solutions du système

$$\begin{cases} 7x + 5y - z = 0 \\ 2x + 2y - 3z = 0 \end{cases}$$

est $\{(13k, -19k, -4k), k \in \mathbb{Z}\}$.

7.2.3 Conclusion

Nous avons vu deux types d'équations diophantiennes qui peuvent être résolues de manière systématique : les systèmes d'équations diophantiennes linéaires, qui se résume a une réduction matricielle, et les équations polynômiales homogènes de degré 2. Dans le cas d'une équation $P(X_1, \ldots, X_n) = 0$ avec $n \geqslant 2$ et $p \in \mathbb{Z}[X_1, \ldots, X_n]$ homogène de degré deux, on commence par étudier l'existence d'une solution non triviale à l'aide du théorème de Hasse-Minkowski. Pour cela, on peut soit utiliser le théorème 11, soit étudier l'équation sur les corps finis et essayer de relever les solutions dans les corps $\mathbb{Q}_p$ avec le lemme de Hensel (sans oublier d'étudier le cas réel). On obtient alors l'existence, ou non, d'une solution non triviale dans $\mathbb{Q}^n$, mais ce projet n'a pas présenter d'algorithme pour calculer effectivement une telle solution. De tels algorithmes existent, un exemple pour le cas à trois indéterminées est donné dans [2]. Partant d'une solution non triviale on détermine un paramétrage rationnel de l'hypersurface d'équation $P(x_1, \ldots, x_{n-1}, 1) = 0$ (après permutation éventuelle des indéterminées) ; ceci est toujours possible dans le cas où P est de degré 2 en faisant l'interscection de cette hypersurface avec des droites de pentes rationnelles passant par le point solution déterminé précédement. Ce paramétrage rationnel nous donne alors les autres solutions.

Bibliographie

[1] J.P Serre,*Cours d'arithmétique*, PUF, Collection Sup "Le mathématicien", 1970

[2] Henri Cohen,*Number Theory Volume I : Tools and Diophantine Equations*, Springer, 2007

[3] Denis Serre,*Les matrices*, Dunod, 2001

[4] François Combes,*Algèbre et géométrie*, Bréal, 1998

[5] Z.I. Borevitch et I.R. Chafarevitch,*Théorie des nombres*, Gauthier-Villard Paris, 1967